World Technology Evaluation Center

WTEC

WTEC Panel Report on

European Nuclear Instrumentation and Controls

James D. White, Co-Chairman
David D. Lanning, Co-Chairman
Leo Beltracchi
Fred R. Best
James R. Easter
Lester C. Oakes
A. L. Sudduth

December 1991

Coordinated by

Loyola College in Maryland
4501 North Charles Street
Baltimore, Maryland 21210-2699

WORLD TECHNOLOGY EVALUATION CENTER

SPONSOR The World Technology Evaluation Center (WTEC) is a companion to the long established Japanese Technology Evaluation Center (JTEC) at Loyola College. WTEC is operated for the Federal Government to provide assessments of European research and development (R&D) in selected technologies. The National Science Foundation (NSF) is the lead support agency. Other sponsors of WTEC and JTEC include the National Aeronautics and Space Administration (NASA), the Department of Commerce (DOC), the Department of Energy (DOE), the Office of Naval Research (ONR), the Defense Advanced Research Projects Agency (DARPA), and the U.S. Air Force.

PURPOSE The steady integration of the European market system and the pressures of competition from worldwide sources in high technology have stimulated the consolidation of European R&D among companies and nations. The resulting trends are for faster paced development of technologies directly competitive with those in the U.S. As European nations and corporations become leaders in research in targeted technologies, it is essential that the United States have access to the results. WTEC provides the important first step in the process by alerting U.S. researchers to state of the art accomplishments in other nations. WTEC findings are also of interest in formulating governmental research and trade policies.

APPROACH The assessments are performed by panels of about six U.S. technical experts. Panel members are leading authorities in the field, technically active, and knowledgeable about both U.S. and foreign research programs. Each panelist spends about one month of effort reviewing literature, making assessments, and writing reports on a part-time basis over a twelve month period. Panels conduct extensive tours of university and industrial research facilities in selected foreign host countries. To provide a balanced perspective, panelists are selected from industry, academia, and government.

ASSESSMENTS The focus of the assessments is on the status and long-term direction of foreign R&D efforts relative to those of the United States. Other important aspects include the evolution of the technology and the identification of key researchers, R&D organizations, and funding sources.

REPORTS The panel findings are presented to workshops where invited participants critique the preliminary results. Final reports are distributed by the National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, Virginia 22161 (703-487-4650). The panelists also present technical findings in papers and books. All results are unclassified and public.

LOYOLA COLLEGE The function of the WTEC staff at Loyola College is to coordinate excellent assessments and to produce reports of the highest professional quality. WTEC helps select topics, recruits experts as panelists, organizes tours of foreign laboratories and industrial sites, assists in the preparation of workshop presentations, and provides editorial assistance for the final report.

Dr. Duane Shelton
Principal Investigator
Loyola College
4501 N. Charles St.
Baltimore, MD 21210

Dr. Michael DeHaemer
Director, WTEC
Loyola College
4501 N. Charles St.
Baltimore, MD 21210

Dr. George Gamota
Senior Advisor to WTEC
Mitre Corporation
Bedford, MA 01730

WTEC Panel on

EUROPEAN NUCLEAR INSTRUMENTATION AND CONTROLS

Final Report

December 1991

James D. White, Co-Chairman
David D. Lanning, Co-Chairman
Leo Beltracchi
Frederick R. Best
James R. Easter
Lester C. Oakes
A. L. Sudduth

This material is based upon work supported by the National Science Foundation (NSF) under NSF Grant ECS-8922947, awarded the Japanese Technology Evaluation Center at Loyola College in Maryland. The Government has certain rights in this material. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect those of the United States Government, the authors' parent institutions or Loyola College.

WTEC/JTEC STAFF

R. D. Shelton, Principal Investigator

Michael DeHaemer, WTEC Director

Geoffrey M. Holdridge, JTEC Director

Bobby A. Williams, Assistant Director

Aminah Batta, Administrative Assistant

Catrina Foley, Office Assistant

Patricia M. H. Johnson, Editor

ACKNOWLEDGEMENTS

This assessment was made possible by the assistance of many organizations which the panel would like to acknowledge. Visits to many sites were necessary to carry out the assessment. In each site visit, the industrial organization visited: received the panel warmly; made available several technical personnel to answer our questions; and recommended written information they considered most appropriate for our study. The quality of the information presented was outstanding. The openness of the discussions with all participants was extraordinary. All of these organizations encouraged the panel's efforts, rather than questioning the reason for an assessment of this kind. These organizations also made written review comments on our draft report. Beyond this, several representatives from these organizations travelled to the U.S. to attend the workshop and give us the benefit of their latest information. The authors are very appreciative of this encouragement and support. Our tasks were much easier in this kind of environment.

We would like to thank the NSF and DOE for sponsoring this study which we think is very important. We would also like to thank the WTEC/JTEC staff for their help in making this study and report successful: Duane Shelton's help in Russia was extremely effective; Geoff Holdridge and Bobby Williams' assistance made the workshop successful; and our sincere gratitude goes to Aminah Batta whose patience and persistence were important for the successful preparation of the final report. Through a subcontract with Loyola, the American Trade Initiatives, Inc (ATI) team consisting of Joe Conn and John Mikula, organized the itinerary for our visits to the European sites; they personally drove us to meetings in some tight situations. The panel would like to express its appreciation to the ATI personnel.

FOREWORD

This is the first report prepared through the World Technology Evaluation Center (WTEC), sponsored by the National Science Foundation (NSF) and coordinated by Loyola College in Maryland. It describes research and development efforts in Europe in the area of instrumentation and control of nuclear power plants for electricity generation. WTEC is an outgrowth of and a companion to the Japanese Technology Evaluation Center (JTEC) which, for a number of years, has published a series of important technology assessments under NSF sponsorship. While JTEC will continue as a channel for evaluating Japanese technologies, WTEC broadens the geographic scope of technology assessment.

Over the past decade, the United States' competitive position in world markets for high technology products appears to have eroded substantially. As U.S. technological leadership is challenged, many government and private organizations seek to set policies that will help maintain U.S. competitive strengths. To do this effectively requires an understanding of the relative position of the United States and its competitors. Indeed, whether our goal is competition or cooperation, we must improve our access to the scientific and technical information in other countries.

Although many U.S. organizations support substantial data gathering and analysis directed at other nations, the government and privately sponsored studies that are in the public domain tend to be "input" studies. That is they provide measurement of expenditures, personnel data, and facilities, but do not provide an assessment of the quality or quantity of the outputs obtained. Studies of the outputs of the research and development process are more difficult to perform since they require a subjective analysis by individuals who are experts in the relevant technical fields.

The National Science Foundation staff includes professionals with expertise over a wide range of technologies. These individuals provide the technical expertise needed to assemble panels of experts who can perform competent, unbiased, scientific and technical reviews of research and development activities. Further, a principal activity of the Foundation is the review and selection for funding of research proposals. Thus the Foundation has both experience and credibility in this process. The WTEC activity builds on this capability.

Specific technologies, such as nuclear instrumentation and control, or telecommunications, or biotechnology, are selected for study by individuals in government agencies who are able to contribute to the funding of the study. A typical assessment is sponsored by two or more agencies. In cooperation with the

sponsoring agencies, NSF selects a panel of experts who will conduct the study. Administrative oversight of the panel is provided by Loyola College in Maryland, which operates WTEC under an NSF grant.

Panelists are selected for their expertise in specific areas of technology and their broad knowledge of research and development in both the United States and in the countries that are of interest. Of great importance is the ability of panelists to produce a comprehensive, informed and unbiased report. Most panelists have travelled previously to the host countries or had professional association with their expert counterparts. Nonetheless, as part of the assessment, the panel as a whole travels to host countries to spend one full week, as a minimum, visiting research and development sites and meeting with researchers. These trips have proven to be highly informative, and the panelists have been given broad access to both researchers and facilities. Upon completion of its trip, the panel conducts a one-day workshop to present its findings. Following the workshop, the panel completes a written report that is intended for widespread distribution.

Study results are widely distributed. Representatives of the host countries and members of the media are invited to attend the workshops. Final reports are made available through the National Technical Information Service (NTIS). Further publication of results is encouraged in the professional society journals and magazines. Articles derived from earlier JTEC studies have appeared in *Science, IEEE Spectrum, Chemical and Engineering News* and others. Additional distribution media, including video tapes, are being tested.

Over the years, the assessment reports have provided input into the policy making process of many agencies and organizations. A sizable number of the reports are used by foreign governments and corporations. Indeed, the Japanese have used JTEC reports to their advantage, as the reports provide an independent assessment attesting to the quality of Japan's research.

The methodology developed and applied to the study of research and development in Japan is now proven to be equally relevant to Europe and other leading industrial nations. In general, the United States can benefit from a better understanding of cutting-edge research that is being conducted outside its borders. Improved awareness of international developments can significantly enhance the scope and effectiveness of international collaboration and thus benefit all our international partners in joint research and development efforts.

Paul J. Herer
National Science Foundation
Washington, DC

TABLE OF CONTENTS

CONTENTS
(Cont'd)

CONTENTS
(Cont'd)

List of Figures

FIGURES
(Cont'd)

List of Tables

x

EXECUTIVE SUMMARY

A study of instrumentation and controls (I&C) technology used in nuclear power plants in Europe was conducted by a panel of U.S. specialists. This study included a review of the literature on the subject, followed by a visit to some of the leading organizations in Europe in the field of nuclear I&C.

KEY FINDINGS

These findings relate to the countries visited and to Pressurized Water Reactor (PWR) nuclear power plants. The countries that the panel visited were France, Germany, Russia, Czechoslovakia, and Norway.

The U.S. is clearly behind in the application of advanced instrumentation and control (I&C) in nuclear power reactors. The September 1991 issue of *Nuclear Engineering International* [Ref. Exec.1] also reflects the status that was observed by the JTEC panel. The contribution to that issue by Electric Power Research Institute (EPRI) describes a recent recognition of the need and initial planning for the use of advanced I&C systems in the United States. The contributions from Japan, France, and Canada discuss the architecture to be used and the capabilities and difficulties of digital systems, including software validation and verification. Those contributions from outside the U.S. are all based on several years of operating experience with advanced I&C in commercial power reactors.

All countries in Europe that operate nuclear power plants, as well as Canada, Japan, and the U.S., are moving toward the use of digital computers, especially microprocessors, in information and control systems. The amount of automation and the role of the operator are under discussion in all countries. The view of the operator's role presently varies by country. In Japan and Germany the move is toward a high degree of automation, whereas in France the emphasis is on computer-generated procedures with the decision to enable being made by skilled operators. In U.S. and Soviet plants, the emphasis is on using digital systems to help the operator identify problems, decide on the appropriate corrective actions, and aid in the execution of those actions.

The U.S. is behind in the development and experience of using digital systems in nuclear plants. France has the most experience with digital safety systems and has built successful automatic control and informational systems, the original design having been purchased from U.S. reactor vendors. Germany has developed

a unique control and safety strategy that automatically moves reactor systems back into the safe operating region. Over a broad spectrum of control failures, both of equipment and from human error, this automatic action is sufficient to minimize the number of scrams, smoothing transients to minimize component stresses, and produces time for operator diagnoses. The system presently involves full digital reactor control, and in the preventive and mitigation area uses semiconductor-based analog equipment, which will be replaced by digital equipment without much increase in functionality.

Europe is ahead in the use of fault diagnosis and signal validation systems. Work on the use of digital information programs for fault management systems in nuclear plants is moving more rapidly in both Europe and Japan than in the U.S.

The hardware for the digital systems used in all countries is by and large from U.S. computer companies, but the lack of deployment of digital systems in U.S. nuclear plants has kept the U.S. behind in the development of experience in the computer system architecture for the instrumentation and control systems in the plants.

In France and Germany, control strategies have been extended to allow nuclear power plants to be used for automatic changes in power to match demands from the utility grid. These capabilities involve improved control of local power distribution changes during transient power conditions.

Instrumentation for nuclear power plants is similar to that in the U.S. in all countries visited by the panel. Some special instrumentation is being developed. For example, a special neutron detection system is under development in France to provide improved in-core and ex-core power density and transient power level information. Germany has pioneered the use of prompt, in-core cobalt detectors for gathering detailed power density information.

The European countries are ahead in the use of computer assisted software engineering (CASE) tools, and they are more advanced in the development of standards.

As a conclusion to the key findings, at the workshop review of the panel's preliminary findings, one final statement was made by a member of the audience:

> The U.S. being behind may not be so bad. Look hard at the mistakes that those ahead have made. Two examples where technology got too far ahead:
>
> 1) The Darlington case in Canada where: a) full cognizance of evolving world standards was not considered in the early development; and b) there were unneeded complexities in the safety system.

2) The N-4 plant problem in France is another example where complexity is a big factor.

In general, the caution of the French and Canadians is attributable to the fact that the programmability of the digital systems can entice the user to add complexities that can evolve into problems. Efforts must be made to maintain simplicity. This problem is often not recognized until the review, quality assurance (verification and validation), and final approval stage.

QUALITATIVE COMPARISONS OF BASIC RESEARCH, ADVANCED DEVELOPMENT, AND PRODUCT IMPLEMENTATION

The panel has made a qualitative comparison of the U.S. nuclear power situation standing relative to the countries visited for status and progress in basic research, advanced development, and product implementation in the seven categories studied, namely: control room design; analog-to-digital transition; fault management systems; control strategies; I&C architecture; instrumentation; and standards and tools. The specific content of these categories is defined in the individual chapters of this report.

As shown in Figure Exec.1, Europe is ahead of the U.S. and moving ahead further in implementation of products in all seven categories, with the possible exception of instrumentation. In the area of advanced development, Europe is also ahead except for architecture and instrumentation. In basic research, Europe is ahead in four of the seven categories; however, for analog-to-digital transition and for instrumentation, the U.S. is about equal, and the U.S. is ahead in architecture . In other words, U.S. computers are being purchased and utilized in all countries that the panel visited, but the development and implementation of the computers for nuclear power plant instrumentation and control is more advanced in Europe and Canada.

EVOLUTION OF AUTOMATION IN NUCLEAR POWER PLANTS

There is a move in every country designing nuclear power plants to improve the plant's availability, safety, ease of operation and/or acceptability by the public and regulators. For the U.S. to make this transition, it is prudent to look at the experiences of other countries and to look at where the design evolutions seem to be headed. The appropriate balance of automation and manual operation is the subject of considerable debate in the U.S. and Europe today. Most researchers agree that today's technology would support digital automation of all of the major systems in a power plant. One of the concerns, however, is how to verify and validate the software required. Recent Canadian experience at Darlington showed how AECL, with many years of experience in computerized protection and control systems, had significant project delays and cost problems

Europe vs. U.S. I&C Summary

	BASIC RESEARCH	ADVANCED DEVELOPMENT	PRODUCT IMPLEMENTATION
Control Room Des.	+ →	+ ↗	+ ↗
Analog-Digital Trans.	0 →	+ ↗	+ ↗
Support Systems	+ ↗	+ ↗	+ ↗
Control Strategies	+ →	+ ↗	+ ↗
Architecture	− ↘	− ↘	+ ↗
Instrumentation	0 →	0 →	0 →
Standards & Tools	+ →	+ →	+ ↗

Jan. 1991

+ indicates Europe ahead

↗ indicates Europe gaining ground

Figure Exec.1. Summary Comparison of Nuclear Power Plant I&C in Europe and U.S.

in the verification and validation of software in their protection system as noted in the key findings. The French recently have had significant project delays at their Chooz-B plant due to problems with their newest control system architecture, although they are very experienced with digital systems in nuclear power.

In the U.S., the transition from today's nuclear control systems to the more automated future designs is likely to occur in phases, as described in an earlier JTEC report (Ref. Exec.2). One of our purposes for this study was to determine where the European concepts were in terms of evolution of I&C. This will be discussed here. The U.S. transition may be described in terms of four levels as shown in Figure Exec.2 and described in Table Exec.1. In Level 1, some of today's analog controllers will be replaced with more reliable digital controllers performing basic proportional-integral-differential (PID) control. This phase of evolution is already under way in the U.S. The Electric Power Research Institute has sponsored some of this work. Generally, digital implementations of control systems on U.S. reactors have been one-for-one replacements of the original analog systems and have not taken full advantage of recent technological developments. Protection systems are also under evolution. Protection systems with some digital features are currently operational at Arkansas Nuclear One Unit 2, Southern California Edison's San Onofre Units 2 and 3, Arizona Public Service's Palo Verde, and Louisiana Power and Light Waterford Unit 3. Level 1 will include essentially automated (computerized) data management at a plant. This has been implemented to a limited extent now in the U.S. LWRs. As the chart shows, the panel thinks that U.S. LWRs are in the beginning of Level 1 and that the French plant Bugey is a little further advanced, but also in Level 1. The Japanese Tokyo Electric Power Company's Kashiwazaki-1 and -2 are, in the view of the panel, more advanced and are at the interface with the next level of transition.

Level 2 of the predicted U.S. transition will include automation of routine procedures like plant startup, shutdown, refueling, load changes and certain emergency response procedures. Significant assistance will be given to the operator through computer-based expert systems and control room displays of plant status. Control will be implemented with digital technology, using predetermined strategies selected from several options. The newly completed Canadian plant Darlington is placed in this level. The newest German plant, ISAR-II, was placed in this category; this plant uses analog technology for control and protection systems while computers and advanced graphical displays are used in the information system. The very high degree of automation of this plant, and the lessons learned/intelligence built into the "limitation system" of the ISAR plant, seemed to warrant placement of this concept on the border of Levels 2 and 3. Also in Level 2 are the U.S. Advanced Light Water Reactor (ALWR), as defined in the EPRI Requirements document, and the newest French plant (the N4 class). Since neither of these plant types is operational, the diamonds representing them on the chart are empty, rather than solid, whereas the German plant is operational and is represented by a black diamond on the figure.

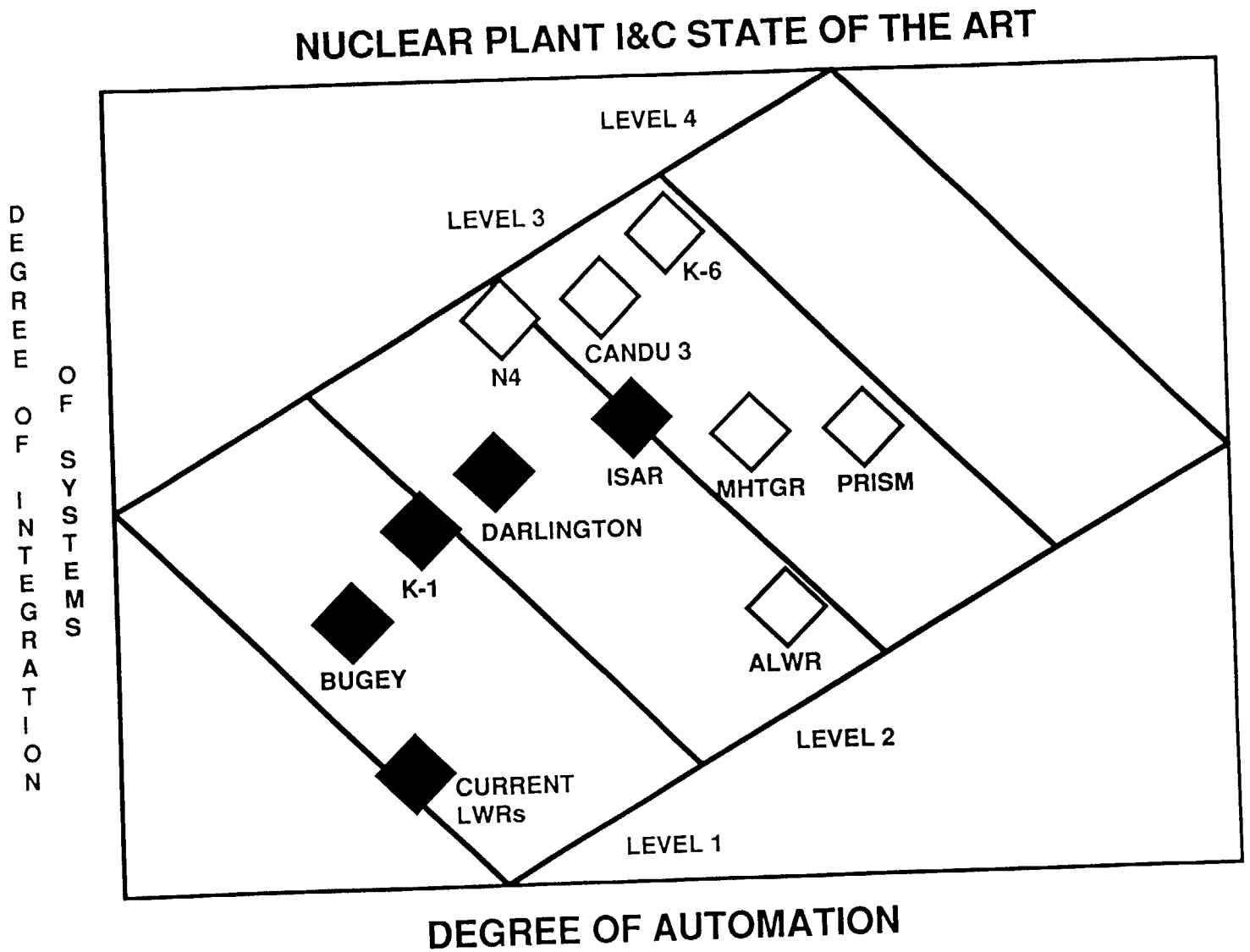


Figure Exec.2. Nuclear Plant I&C State of the Art

Table Exec.1

Phases of Evolution in I&C for Nuclear Power Plants

Level 1	Level 2	Level 3	Level 4
mostly manual control	automation of normal ops	automated fault management	full plant automation
analog controls relay logic	digital control of some processes	total digital control	integration through information network and common db
disintegrated systems	rule based operator behavior	full integ. control and monitoring for power prod.	integration of all O&M functions
rule and skill based operator behavior	fault tolerant architectures	knowledge based operator behavior	operator as supervisory
no fault tolerant architectures	operator support for fault management	expert systems as advisors	robotics and remote systems
		advanced control strategies	expert control

Level 3 is a significant advance toward automation with the operator interacting with and monitoring an intelligent, adaptive supervisory control system. Smart sensors will be expected to validate their own signals and communicate with fault-tolerant process controllers. At this level, the process controllers will be able to reconfigure the control logic to meet the operational objectives selected by the supervisory control system. Control strategies will be adaptive, and very robust to off-normal conditions. Completely automated plant designs with plant data bases will be available to the control system and the operator. Operational experience of all plant systems and components will be tracked in an automated data base. The information system will recommend maintenance schedules and outages to the operator. Human performance modeling will have permitted good allocation of function decisions in a way to keep the operator motivated and informed about plant status. Advanced LMR (PRISM) concepts and MHTGR concepts being studied by the U.S. DOE will have these capabilities. The newest Canadian concept, the CANDU 3, is placed in this category, as is the Japanese Advanced Boiling Water Reactor (ABWR), under construction now at Kashiwazaki as Units 6 and 7. Several other countries have R&D organizations working on individual systems which have some of the characteristics mentioned here, but have not integrated the concepts into total plant designs.

Level 4 would be characterized as total automation of the plant, with an intelligent control system aware of operational status and in interactive communication with the operator to keep him apprised concerning any degraded conditions, likely consequences of these conditions, possible (recommended) strategies for minimizing deleterious consequences. By this time plant designs will have most functions automated and robotized including maintenance and security surveillance.

The control and information system will be an integral part of not only the total plant design, but also the national network of commercial power plants. The control system computer will learn from the network relevant information concerning other plants and component operational experience and will alert the operator if that experience is relevant to his plant. No U.S. design has gone this far in incorporation of advanced technology and automation. The Japanese Frontier Research Group on Artificial Intelligence is working on conceptual definition of a plant of this type.

In the evolution of higher levels of automation, the designers will be trying to improve all aspects of nuclear power plants, including safety and reliability. The progress in all countries should build on successes and experiences in other countries. This report highlights some of the most significant technical achievements in automation of nuclear plants in the countries visited.

REFERENCES

1. Reed Business Publication Group, *Nuclear Engineering International*, September 1991, Vol. 36. No. 446, pp. 22-40.

2. K.F. Hansen et al., "JTEC Panel report on Nuclear Power in Japan," October, 1990, available from National Technical Information Service, U.S. Dept. of Commerce, NTIS Report # PB90-215724.

CHAPTER 1

INTRODUCTION

James D. White and David D. Lanning

Control and instrumentation systems might be called the "brain" and "senses" of a nuclear power plant. As such they become the key elements in the integrated operation of these plants. Recent developments in digital equipment have allowed a dramatic change in the design of these instrument and control (I&C) systems. New designs are evolving with Cathode Ray Tube (CRT)-based control rooms, more automation, and better logical information for the human operators. As these new advanced systems are developed, various decisions must be made about the degree of automation and the human-to-machine interface. Different stages of the development of control automation and of advanced digital systems can be found in various countries.

The purpose of this technology assessment is to make a comparative evaluation of the control and instrumentation systems that are being used for commercial nuclear power plants in Europe and the United States. This study is limited to Pressurized Water Reactors (PWRs). Part of the evaluation includes comparisons with a previous similar study assessing Japanese technology.

The panelists involved in this study were chosen to represent a spectrum of U.S. experts in the area of control and instrumentation. Representatives from national laboratories, commercial industry and industrial research organizations as well as from academia were invited to participate. A list of the panelists' names and titles is provided below. More complete information including biographical sketches of each panelist is given in the Appendix A.

James D. White (Co-Chairman)
Oak Ridge National Laboratory

David D. Lanning (Co-Chairman)
Massachusetts Institute of Technology

Leo Beltracchi
U.S. Nuclear Regulatory Commission

Fred R. Best
Texas A&M University

James R. Easter
Westinghouse Energy Center

Lester C. Oakes
Electric Power Research Institute

A. L. Sudduth
Duke Power Company

The procedure for the preparation of the final report consisted of seven steps:

1) A literature search was conducted to assess the recent published information that was available from each of the countries to be visited.

2) Based on the published literature plus some personal knowledge from panelists, a listing of places, companies and individuals was prepared for potential contacts and site visits.

3) Arrangements were made for the panelists to visit European sites; after initial contacts were made, the hosts in each country were helpful in assuring that the proper people were contacted to provide the desired technology reviews.

4) The panel visited 22 I&C sites over a two-week period in December 1990.

5) The panel delivered a preliminary oral report of its assessment at a workshop held at the NSF offices in Washington, D.C. on January 30, 1991.

6) Draft chapters of the final report were prepared and reviewed by the panelists, and then the draft report was sent to the hosts in each country in May 1991.

7) Comments and corrections were received from the hosts and were incorporated into the final report.

Figure 1.1 and Table 1.1 indicate the sites visited by the panel. Arrangement and scheduling for these visits were made by American Trade Initiatives, Inc. (ATI). The panelists are truly appreciative of efforts by the staff from ATI and of the gracious response of the hosts who received us in each of the countries. The scheduling had to be tightly coordinated, and it all went extremely well.

To perform this review and technology assessment, each panelist agreed to take a particular topical area as a primary responsibility and also agreed to take secondary responsibility to assist another panelist in his primary area. The report was then reviewed by the hosts or their representatives for each country.

In the following overview and chapters, the name of the panelist with the primary responsibility is shown as the author for the chapter.

Chapter 2 Role of the Operator and Control Room Design (James R. Easter)

The Search for the proper balance between the human operator and the amount of automation is continuing. In Europe, the balance is moving toward more automation, more information on CRT screens, and the use of multi-function controls. Research in analysis of human error is most advanced in the USSR.

Chapter 3 Transition from Analog to Digital Technology (Lester C. Oakes)

The availability of digital systems offers an attractive flexibility for control system designs, and lack of analog replacement equipment combines to push all countries toward more use of digital systems.

Chapter 4 Computerized Operator Support Systems for Fault Management (A.L. Sudduth)

Interest and research in fault management is widespread, including signal validation (in use today) and research on fault detection, diagnosis, mitigation, and success assurance. These systems are being developed in both Europe and the U.S., but deployment in power plants is more advanced in Europe.

Chapter 5 Control Strategies and Techniques (David D. Lanning)

Automation is already being used over a wider operating range in Europe than in the U.S., and more implementation of digital systems for control and safety systems is in progress. There is a surprising amount of automation in the German Konvoi plants.

Chapter 6 An Investigation of Nuclear Power Plant I&C Architecture (James D. White)

Distributed microprocessors are being used or designed especially in France and Canada. These are to be used in control and information systems with fault-tolerant combinations of programmable digital systems.

Chapter 7 Instrumentation (Fred R. Best)

New developments in detectors and attached instrumentation are in progress at some research centers, but not many new instruments have been employed on nuclear power plants. An example of an interesting instrument is the in-core detector being developed in France.

Chapter 8 Computer Standards and Tools (Leo Beltracchi)

Many tools for software engineering have been developed and general standards have been considered. However, complete integration of tools into the development cycle remains an important but difficult goal to reach. The panel found that the use of tools is much more prevalent in Europe than in the U.S.

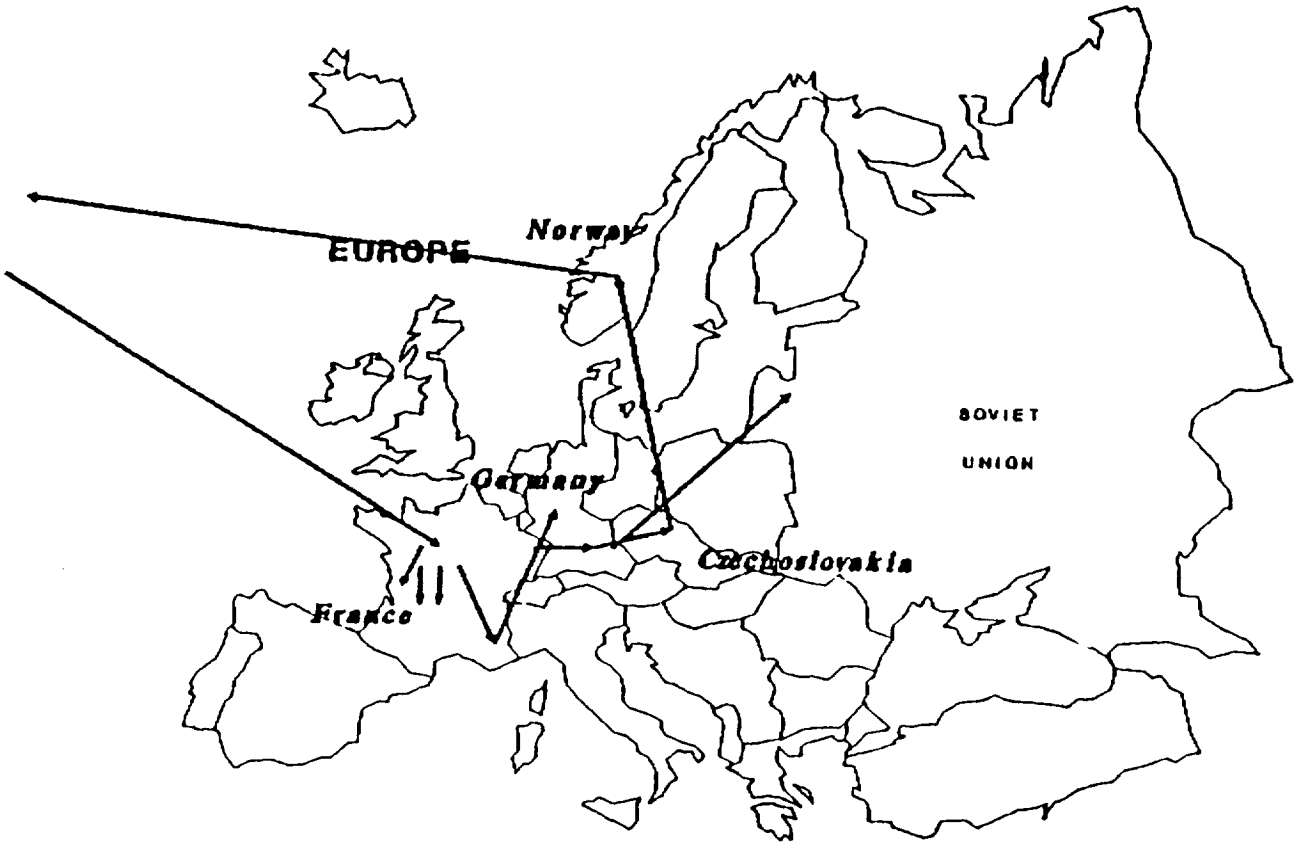


Figure 1.1. Map of Places Visited by the Panel

Table 1.1

PLACES VISITED BY THE PANEL

FRANCE	
Framatome	La Defense Paris
CEA-CE	Saclay
CEGELEC	Paris
CEA, IPSN	Paris
EDF	Chatou
EDF SEPTEN; BUGEY Training Center and PWR Power Plants	Near Lyon
CEA Cadarache	Near Marseilles
Merlin Gerin	Grenoble
CORYS	Grenoble
GERMANY	
KFK	Karlsruhe
ABB	Heidelberg
KWU-Siemens	Karlstein
GRS	Garching/ Munich
ISAR-II Power Plant (KONVOI)	
CZECHOSLOVAKIA	
SKODA	Pilzen
Ministry of Economics	Prague
Nuclear Research Institute	Rez
Dukovany PWE Power Plant	Near Brno
U.S.S.R.	
I.V. Kurchatov Institute of Atomic Energy	Moscow
VNIIEM	Moscow
Institute of Control Problems	Moscow
NORWAY	
Halden Research Laboratories (OECD)	Halden

CHAPTER 2

ROLE OF THE OPERATOR AND CONTROL ROOM DESIGN

James R. Easter

INTRODUCTION

This chapter presents an assessment of the current state of the art in Europe, Eastern Europe, and the Soviet Union in the application of modern computer technology to control room requirements for the next generation of nuclear power plants. In addition, this chapter compares nuclear plant control room design in the countries visited by this panel with that in Japan as reported in the panel report, *Nuclear Power in Japan* (Ref. 2.1), and with that in the United States in the experience of the panelists.

In order to keep the project manageable, the panel visited research and development establishments in a limited number of countries: France, Germany, the Soviet Union, Czechoslovakia, and Norway. The panel's assessment is based upon a literature review of work performed in these countries; visits to a number of their leading research and development groups; and study of material provided by organizations the panel visited.

WHAT ROLE FOR THE OPERATOR?

In order to assess or evaluate the design of a process plant control room, it is necessary to understand the objectives and the reasoning behind the design. Critical to the design of any product is understanding the end user and how he/she expects the product to perform. In the case of the control room of a nuclear power plant, the end user is the operating staff that will man that room. How that room is expected to behave and the number of crew members required to make it happen, however, is usually dictated by the plant's owner or utility.

Because the nuclear power industry is dealing with a highly concentrated energy source that can, if mishandled, have disastrous consequences for the owner, the public, and the environment, the utility industry worldwide is actively seeking to improve operator reliability. Several analyses of mishaps in the process industry in general show that most accidents can be traced to human error of one form or another (Refs. 2.2, 2.3). Not all of these are the result of operator error. Many are the result of faulty maintenance, and some are the result of basic design flaws; all are human errors none the less. For the designer of nuclear power plant control rooms, however, the emphasis is clearly on improving the reliability of the operator in the monitoring and control of the plant's nuclear and thermodynamic processes.

Figure 2.1 is a simple illustration of the three approaches that can be taken for improving operator reliability in a process plant control room. What follows is a discussion of each of these approaches and then an examination of which approach or combination of approaches is being addressed by the control room research, development, and design organizations in each of the countries that this panel visited.

Follow Procedures

Traditionally, operator reliability has focused on developing and enforcing strict procedures and on the subsequent training of operators to know how to follow them. This approach has been developed by trial and error over several centuries of human endeavor in the manufacture and use of hazardous materials such as military munitions. This approach is best used for situations where the timing of the process is under the direct control of the operator, i.e., a user-paced process. Here, operator mistakes can be recovered without any amplification by the process. In situations where the timing is determined by the process, i.e., a system-paced process, operator mistakes are usually exacerbated by the process and recovery is much more difficult.

In addition, this approach expects complete knowledge on the part of the procedure designer relative to how to respond to all of the possible permutations and combinations of conditions that the process could possibly exhibit. Failures to perform to this level are discovered after the fact--that is, after a mishap occurs. Correction is made by reactively modifying the procedure and instituting more operator training. Until the development of modern electronics and automatic control theory, this was the only approach available to address the problem of operator reliability.

Automate Everything

World War II greatly accelerated the development of the equipment and the understanding for automating real-time processes. Today, modern computer

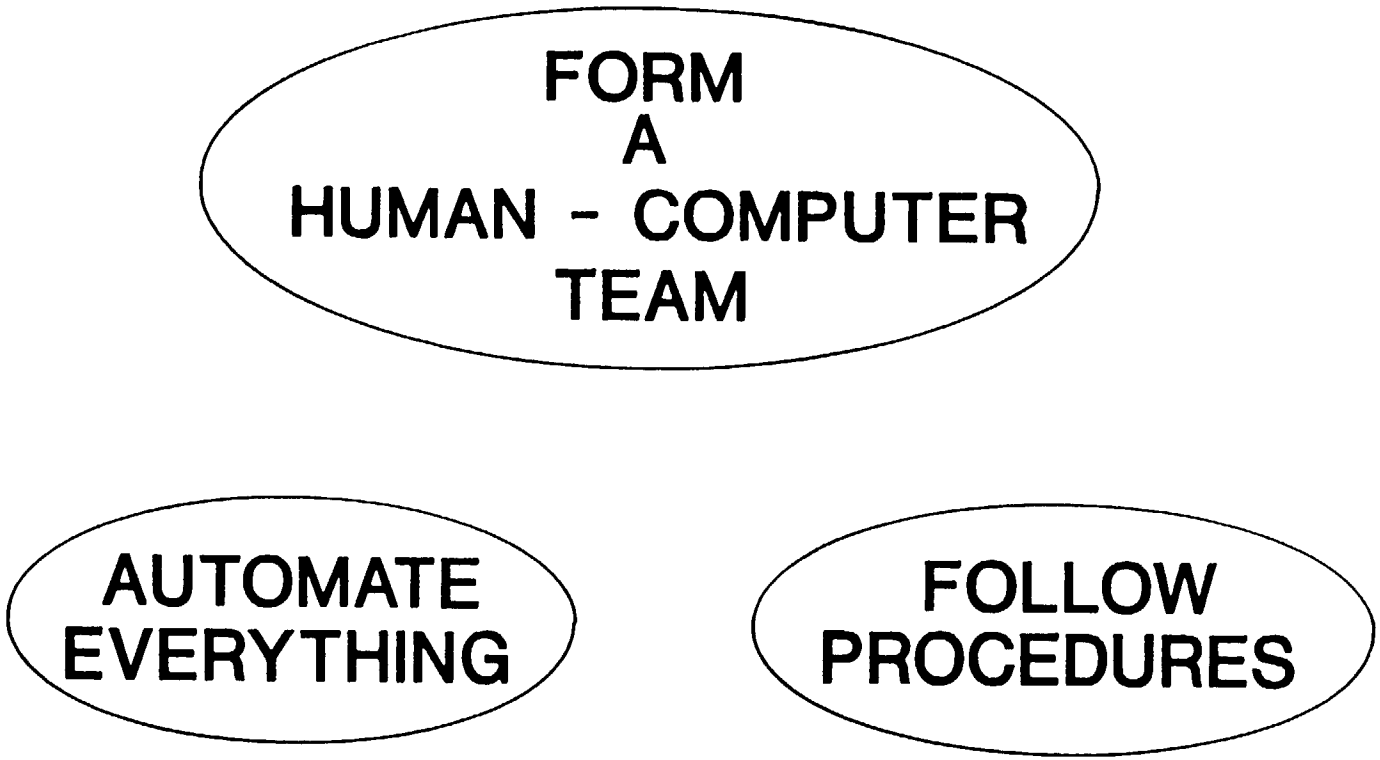


Figure 2.1. What Role for the Operator?

technology and control theory make it possible to envision, if not in fact to build, totally automated plants. This approach attempts to improve operator reliability by removing the operator from any part of the process control activity. The plant owners and the public would then depend solely on electronics for process performance and safety.

Form a Human-Computer Team

The last decade's astounding advances in computer technology have made it possible for control room designers to envision yet a third approach. This approach is to establish a human-computer team, allocating cognitive and physical activities appropriately to each partner. This approach extends the nuclear industry's traditional "defense in depth" philosophy to the design of nuclear control rooms and to the treatment of operator error. With a human-computer team, not only is there some redundancy in the decision-making activity, but also there is diversity in the decision-makers and in their approaches.

Emphasis is placed upon creating an atmosphere of dialogue between the partners, each having the ability to cross-check the decisions and actions of the other, thereby encouraging an interlocking web of support in terms of avoiding, finding, and compensating for errors and failures.

Strengths and Weaknesses of the Three Approaches

The above discussion implies that each of these approaches is unique and independent; in fact, they are not. Mixtures of any two or even of all three are more often found than the pristine application of only one. Furthermore, there is currently scant evidence to indicate that one or the other or even a specific mixture of these approaches is more effective than another at improving human operator reliability.

Follow procedures. The approach that focuses on comprehensive procedures and exhaustive training is the best understood and the most often used. Witness the major revisions in these areas mandated by the U.S. Nuclear Regulatory Commission (NRC) after the March 1979 incident at the Three Mile Island plant. This is probably the major strength of this approach: people and organizations know how to do it. Its major weakness is that the responsibility for process performance is in the hands of the procedure writers, not the plant operators. The operator becomes, in the extreme case, merely a biological robot who is not required to understand anything, merely to be able to read the procedure and to execute the required actions.

Another problem with this approach is that, alone, it is incapable of addressing the issue that as processes have become more complex, the ability of humans to

carry them out in a timely manner has become a limiting factor in process performance. Some form of automation is required to improve the speed and to handle complex control sequences.

Automate everything. The major strengths of automation are its abilities to be constantly vigilant, to analyze large quantities of process data, to create more appropriate control variables from them, and to execute actions and sequences of actions more quickly than can a human. What it cannot do very well is to reason about situations for which it was not designed. Humans are better at that.

Again, the questions are what relationship does a human operator have with the automata in this approach, and how does the answer to that question affect the design of the automata and of the human interface to it?

As the process becomes more and more automated, the operator clearly has fewer physical tasks to perform, and the nature of mental activity changes. In the past, he/she attempted to carry out the process parameter analysis in order to determine the correct control action, tasks that the automata now performs. With the automata, the operator's role becomes one of **managing** the activities of the automata. This change in role implies changes in the required supporting resources (i.e., the process data being presented, the procedures, the nature of the process controls, etc.) that the operator uses to carry out those activities; indeed, it changes the very image that the operator has of the job itself (Ref. 2.4). While automation and control theory are not new subjects, the realization that people must still be involved and the effects of automation on their tasks are subjects only now being addressed by the research and development community.

Form a human-computer team. The third approach can be viewed as an extension of the previous one in the sense that computers play a very significant role in the realization of the man-machine (human-plant process) interface, including that of automating the control of plant processes. However, the central role of the computers and the relationship between them and the operators is somewhat different than when designed to independently control the process. The focus of this approach is to provide a "holistic" environment that coordinates the interface in such a way that the dialogue between man and machine becomes (from a human point of view) natural and convenient and covers all of the necessary perspectives and resources required for monitoring and controlling the processes.

The strength of this approach is that it attempts to remove some of the known sources of human error. In current control rooms, there is interpretive mental workload caused when an operator must move from one media of information to another (such as from control board lights and meters to paper procedures) or from one representation of the problem space to another (such as from alarms to procedures or from procedures to process parameter displays). By properly

computerizing these resources, much of this mental work load can be greatly reduced, if not eliminated. Also, it is possible with computers to ensure that the process data is presented in its proper and relevant context, rather than expecting the operator to mentally synthesize the context.

This approach recognizes that the responsibility for process performance is shared between the operators and the designers of the computerized systems by creating an environment that encourages cross-checking and the exchange of data and viewpoints between humans and computers. The weakness is that while these are enticing objectives, they are very new. There is very little practical experience with systems designed and constructed with such objectives in mind. As a result, there is little concrete evidence to date that such an approach really does improve operator reliability.

It is within the framework of these three approaches to the roles of operator and automation in control room design that this panel reviewed and evaluated the nuclear power plant control room technologies of France, Germany, the Soviet Union, Czechoslovakia, and Norway. The summary of the assessment includes a comparison with the control room technologies of Japan and the United States.

COUNTRY-BY-COUNTRY ASSESSMENT

The French Program

A control room with operator workstations and a large wall mural/mimic is being installed in the new 1400 MWe N4 plant being built at Chooz, France, by the French national utility, Électricité de France (EDF). A full-scope simulator (Figure 2.2) has been built at the EDF Bugey plant site near the French city of Lyon and is currently being used for operator training and human factors design validation tests (Ref. 2.5). Commercial operation of the N4 plant is currently scheduled for the 1995-6 time frame.

This control room is a most ambitious and aggressive design and is currently the industry's trend setter. While other countries the panel visited are heading in this same direction, the N4 control room has by far the most maturity, design work having begun in the early 1980s. Visually, this control room is markedly different from any currently existing nuclear power plant control room. Figure 2.2 shows two workstations joined together. Each workstation can be used to control the entire plant, or the work can be shared between the two. A third identical workstation will be used by the supervisor for monitoring and, in case of failure of one of the other workstations, for control. All process data is displayed on cathode ray tube monitors (CRTs) embedded in the vertical surface of each workstation desk, as are the operating procedures and all of the alarm messages.

Process control is accomplished through the use of touch screens on those CRTs embedded in the horizontal surface of the desk. In other words, the control board is completely computerized for all modes of operations. Emergency Safeguards equipment can also be manually actuated at the systems level through hard-wired push buttons located on that portion of the desk between the two workstations. In case of complete computer system failure, a traditional hard-wired analog control panel for component level safety equipment is located at the back of the control room.

From an ergonomic standpoint, this control room design is intended to reduce, if not eliminate, certain types of operator error. The use of state-of-the-art computer graphic display equipment and multifunction control devices permits the operator to have an interface with the process by bringing the data and the controls to the operator in a form that is immediately useful. The computer system can collect the process data and can develop new, synthetic variables from it. Such systems can group appropriate data together to form the proper context in order to help the operator better understand the data, and can also group process data appropriately with the process controls. All of these tasks in traditional control rooms required the operator to physically go and find data, mentally perform any synthesis and/or grouping, and then locate the proper controls. Such a work load is obviously prone to both physical and mental errors, and it is time-consuming, thus permitting an errant process to further exceed its bounds, all the while increasing the operator's anxiety level.

The French view of the operator's role in the control room is that he/she is there to follow procedures. The design, organization, and navigation of the CRT display set is based upon the organization and content of the operating procedures. Similarly, the alarm message display, suppression, prioritization, and organization are also based upon the procedures.

Currently, the display monitors do not use "windowing" technology, so a display is created to occupy a full monitor screen. When this author first visited the N4 simulator, in the summer of 1986, EDF had created a library of 10,000 displays. In the fall of 1990, when this panel visited the simulator, the library had grown to 17,000 displays. At first glance this seems like an extraordinarily large number of displays. However, when one considers that a nuclear power plant can have 3000 alarms (each needing to display a trigger logic and a response procedure) 1,000 or so piping and instrumentation drawings (each of which contains 2 to 4 times more data than can be viewed on a single monitor display), and several feet of procedures when in paper form, the number of displays is not so astonishing. What is astonishing is the fact that they have been able to do it with a reasonable amount of manpower. This is a tribute to the effort that EDF has put into

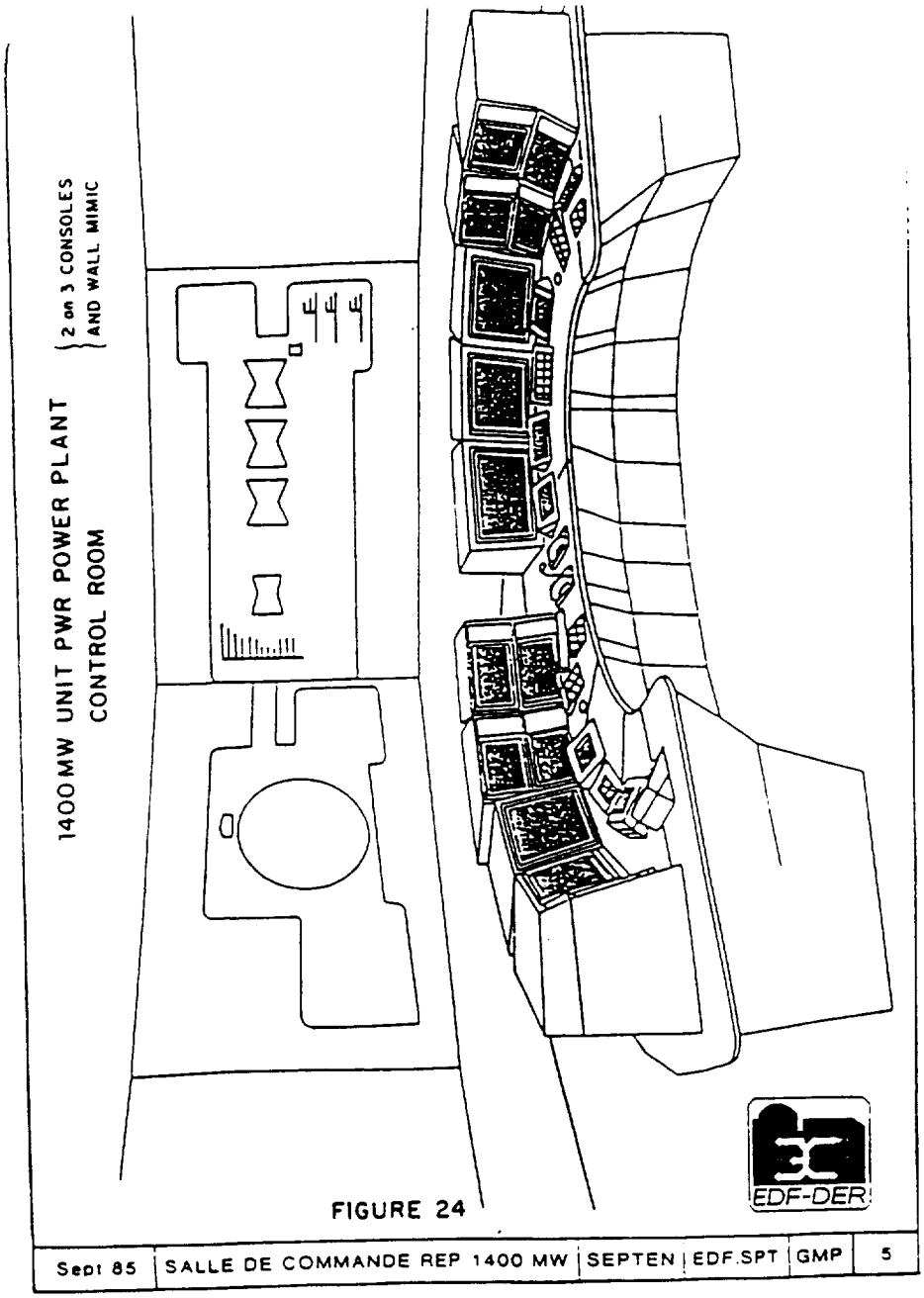


Figure 2.2. The French N4 Control Room
(Courtesy of Electricite de France)

computerizing the entire plant database and to their development of computerized tools for performing the display design and programming process. Only now are American nuclear power plant manufacturers beginning to adopt such tools.

The German Program

The Germans have placed a great deal of emphasis on limiting the consequences of operator action through the use of automation. They have developed and applied to their current plants a sophisticated "limitation system" that architecturally lies between the automatic control system and the plant safety and protection system. (A more detailed discussion of this automatic system can be found in Chapter 5.)

The German response to the March 1979 incident at the TMI-2 plant has been to continue to move steadily ahead using I&C to limit the consequences of operator action with the limitation system and to provide the operator with some additional systems level automation and with sophisticated on-line diagnostic tools. The Germans have only recently developed a set of "symptom-based" emergency procedures such as have been developed in the United States, France, and Japan. They have yet to develop and install Safety Parameter Display Systems (NUREG-0696) or Technical Support Centers although the display system for the KONVOI plants have been analyzed for its SPDS content (Ref. 2.6). They also have not, as yet, adopted and applied the "human factors" discipline (for example, see U.S. NRC NUREG-0700 or NUREG-0800) as many other countries have done. The government-sponsored research facility Gesellschaft fur Reaktorsicherheit (GRS), however, is beginning to pick up the thread of these technologies. This R&D organization is moving to establish expertise in these areas and is interested in seeing these technologies applied to German plants.

Figure 2.3 shows the layout or "footprint" of the control room of the ISAR plant, a 1300 MWe plant located on the Isar River near the city of Munich. This control room, while rather traditional in appearance was licensed on the basis of a conventional control room design, and currently contains an example of nearly every I&C product available in the nuclear power plant market today. It has a large quantity of diagnostic equipment and the component instrumentation to support it. While the control room process parameter display is still focused on the traditional analog meter technology, there are a large number of full-color, high-resolution graphic CRTs. The displays reflect careful thought in their design and presentation and are aimed at helping the operator understand what all the automatic systems are doing.

While there does not appear to be a great deal of emphasis in Germany on the idea of "cockpit" or workstation-type control rooms such as the French N4 design, the German reactor vendor Siemens/Kraftwerke Union (Siemens/KWU) is

performing research and development on such a design (Ref. 2.7). The research appears to be focused more on "how do we build such a room" rather than on "what should we build."

The discussion revolves more around such things as hardware architecture and building a reliable computer system than around what the operator's role is or how that may influence the content and organization of the workstation or the displays.

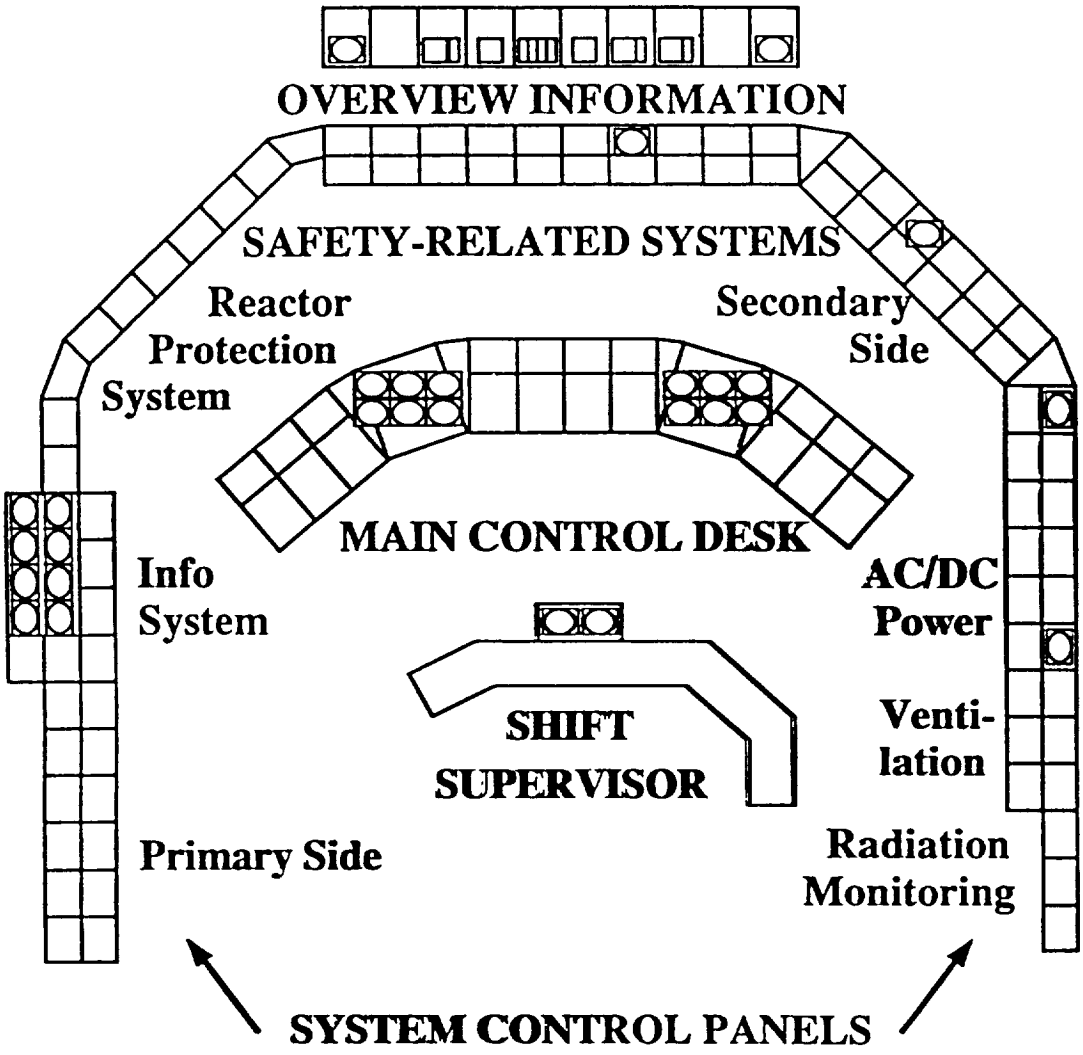
German R&D facilities have been pioneers in the use of computer technology for the purpose of disturbance analysis and diagnostics. This research is highlighted by the activities of GRS, beginning with its development and testing of the STAR System (Ref. 2.8) in the early 1980s and more recently has been generalized in the direction of on-line realtime expert-systems.

A commercial research and development organization, ABB Corporate Research Heidelberg, has been performing "cutting-edge" work in the research and development of knowledge-based support systems for process control room operators. While the current applications of its work are in fossil power plants, the research is directly applicable to nuclear plants as well. This project, titled GRADIENT (graphical dialogue environment), is supported by the ESPRIT project of the European Economic Community (EEC) and was reported to the National Science Foundation in some detail by Dr. Woods (Ref. 2.9).

Briefly, the GRADIENT project is aimed at investigating the use of knowledge-based systems and at enabling the operator to conduct an intelligent graphical dialogue with the machine supervision and control system, supported by a graphical expert system. Among its many features, GRADIENT includes capabilities to model user activities and to recognize errors to help improve operator process control error detection and correction. In addition, its subsystems are intelligent about how to present data, given the user and the plant context. The displays are customized "on-the fly" to the context and user-desired perspective, rather than being completely preformulated and formatted in advance (Refs. 2.10-2.13). (Additional discussion on the contribution that GRADIENT is making to diagnostics and fault management can be found in Chapter 4.)

The Soviet Program

The bulk of the information about Soviet work in the area of control room design was collected in personal communications at a series of meetings at the Kurchatov Institute in Moscow. The Soviets publish little in Western technical journals, and what publications are available, including those given to the panel during these meetings, are almost always in Russian.



Control Room for PWR Konvoi Plants, (KWU)

Figure 2.3. The "Footprint" of the German ISAR Plant Control Room
(Courtesy of Siemens/KWU)

Historically, Soviet work in psychology and applied psychology has been of a high caliber. Based upon the presentations of Soviet scientists and engineers that panelists heard at the Kurchatov Institute, their research into human learning (short-term memory and learning patterns) is now providing a foundation for improvements in control room design.

In recent years, the Soviets have done thorough work analyzing the causes of plant problems resulting from I&C and human error. One of their conclusions from these analyses is that 50 percent of the problems are caused by "high-level reasoning devices," namely, automatic controllers and/or humans; and 50 percent are caused by "low-level devices," such as sensors and data acquisition systems.

As an example of Soviet applied research into causes of operator error in nuclear power plants, a presentation was made to panelists on a series of controlled experiments with operators on simulators that used statistical methods for the analysis and the presentation of the results. U.S. investigators have found that this type of experiment in full-scope simulator tests is difficult to do because of the very large number of hard-to-control psychological variables that can affect the validity of the quantitative results (Ref. 2.14). The Soviet studies were augmented by the more typical methods of examining and analyzing abnormality event reports and of using sophisticated questionnaires and interviews with operators (Ref. 2.15). The results of this specific set of tests has led the Soviets to conclude, among other things, that all of the necessary plant information relative to the operator's tasks needs to be included in a hierarchial display set of no more than two to three levels.

Other analyses have led the Soviets to conclude that, for humans, abnormalities are always surprises, and therefore, the human response tends to exacerbate the abnormality. This conclusion leads Soviet designers to the position that they want the role of the operator in the control room to be one of supervision and management of automatic systems, not one of being an integral element in the "action-taking" response to the abnormality. This is a similar conclusion to the one reached by the investigators of the March 1979 incident at TMI-2 (Refs. 2.16, 2.17). With the exception of the United States, the Soviet Union is the only country in the knowledge of the panel that has an explicit position based upon or in some sense derived from scientific evidence as to what the role of the operator in a nuclear power plant control room should be.

While their fundamental research is of the highest caliber, the Soviets have only recently begun to apply the results. As far as the panelists could tell, these applications have been focused upon backfitting improvements into existing, operating plants. There was no specific evidence of a new control room design, although panelists did see evidence of design work on very sophisticated

computer system architectures and networks (see Chapter 6) that would imply that a new control room design is to be forthcoming.

At the Control Problems Institute (IPU), our Soviet hosts showed panelists development work on computer graphic displays and voice synthesis that is aimed at improving the man-machine interface in nuclear power plants. The Soviets are convinced that not nearly enough attention is being given to using the human auditory capacity as a means of conveying plant process information (e.g., alarm messages) to the nuclear plant control room operator.

The equipment being used for this development work appeared to be of a computer generation that is consistent with the IBM XT personal computer. The graphics devices appeared to be mostly of the character graphics type, though some relatively low-resolution graphic CRTs were in evidence. There was no question, however, that Soviet scientists and engineers were getting the most out this technology, usually through the use of sophisticated numerical and approximation techniques.

The panel's conclusion is that Soviet scientists and engineers are laying a solid foundation in cognitive science and engineering for reducing human error in nuclear power plant control rooms. Application is being hampered by the unavailability of modern, sophisticated computer technology.

The Czechoslovakian Program

As with the Soviet program, the Czechoslovakian program is not well published in Western technical journals. This report is primarily based upon the personal communication of panel members with representatives of the nuclear power community in the Czechoslovak Federal Republic.

The Czechoslovakian nuclear power program has depended almost entirely on the U.S.S.R. As a result, until the fall of the Berlin Wall in late 1989, the design and any improvements have been those of the Soviets. However, since then the Czechoslovaks have been moving aggressively to establish their own design and, particularly, their own positions with regard to the application of modern technologies, including those of the West, to their nuclear power program.

The Czechoslovaks' efforts to improve nuclear power plant control room operator reliability are currently focused on acquiring or building full-scope plant simulators for operator training and for performing engineering analyses of plant behavior. The idea is to subsequently improve plant operating and emergency procedures.

The Czechoslovaks are also moving toward more plant automation, particularly in the form of systems level automation. They have a very explicit desire to leave

the expert control decisions in the hands of the operators, based on their view that the operator is ultimately responsible for plant operations. The Czechoslovaks are aware of the worldwide efforts to improve operator reliability through application of modern computer technology; however, they believe that their currently limited resources can best be focused on better operator training and better understanding of plant performance, resulting in better procedures. They wish to pursue these other types of improvements in the future.

The Norwegian Program (OECD Halden Project)

The Halden Project, located in Halden, Norway, is a recognized world leader in the research of improved human-computer interface design for application to the control rooms of nuclear power plants. The Halden Project is a research organization sponsored by the Organization for Economic Cooperation and Development (OECD) and funded by member countries and organizations worldwide. All members have the right to apply the results of the research in a manner of their choosing. The results of Halden-developed human-computer systems are often applied in a "test-bed" sense in the Loviisa plant in Finland. This provides a level of credibility to the Halden work that is often difficult to achieve by other advanced design and development organizations.

The emphasis in Halden research is to develop effective computerized operator support systems that support rather than replace the operator in performing assigned tasks. In the 1980s, the research focused on individual support systems, such as an advanced alarm system, a computerized procedures system, and the development of methods for creating effective graphics. Recently, however, the focus has moved to the investigation of how best to coordinate such resources and to form them into an effective control room (Ref. 2.18).

SUMMARY AND CONCLUSIONS

With the exception of Czechoslovakia and the Soviet Union, every country that was reviewed in this study is working on a cockpit style of control room that is based upon state-of-the-art computer technology. To this list of countries can be added Japan and the United States. While this approach to the hardware of the operator's workstations seems to be universally appealing, the definition of the operator's role in such a design and the subsequent definition of how the workstations behave in response to that role vary considerably with country and culture. Figure 2.4 is a repeat of Figure 2.1 with the addition of the panel's estimate of where each of the countries considered in this study lies with respect to its definition (either explicit or implicit) of the operator's role in the control room.

The United States, the Soviet Union, and the Scandinavian countries appear to be the only ones making a concerted effort to include the emerging discipline of cognitive systems engineering into the design of new control rooms. While the United States is a very active participant in this area, if not in fact the technology leader, all of the countries in question but Japan are making contributions to the academic level of understanding of the issues; Japan appears not to recognize the discipline of cognitive psychology. However, in the view of the panel, only the United States, the Soviet Union, and the Scandinavians are actively working at bringing this technology out of the laboratories and making it useful to the reliable production of electric power by applying it to the design of control rooms for the next generation of nuclear power plants.

Finally, the panel observed a definite shifting in the influence that U.S. standards writing organizations have over the design and construction of control room facilities. In the past, because the nuclear power plant technology was fundamentally a U.S. technology, our standards institutions were, in effect, the writers of international standards. Three changes have occurred in the last fifteen years in the area of nuclear power plant control room design. The first change is that the nuclear power plant technology is no longer strictly an American technology. This is probably to the credit of the United States, which has willingly shared its expertise with other countries. A significant fraction of the world's population is now benefitting to some degree from U.S. nuclear power technology, but the countries that have accepted its benefits have also sought to understand and to adopt it as their own. This has created experts in these countries (particularly in the area of plant operations) that are now asking to have an impact on the standards for the control room designs of the next generation of nuclear units.

The second change is that because the United States is not currently building new nuclear plants, the perceived level of practicality of our proposed designs, and thus of our standards, is much lower now than it was. Worldwide, utilities that are contemplating new nuclear unit construction are turning from the United States and are seeking experience from countries that have active nuclear construction programs such as France.

This has led to the third change; namely that, because we have built no new designs in the last fifteen years, our standards are obsolete, particularly those related to the very fast-moving technology of modern computer system design as applied to nuclear power plant control rooms. Furthermore, without construction programs, there is little motivation in U.S. standards organizations to update their standards. As a result, the new standards currently being developed that will guide the design of the next generation of nuclear power plant control rooms are being drafted by international organizations such as the International Electrotechnical Commission (IEC) and the International Atomic Energy Agency (IAEA).

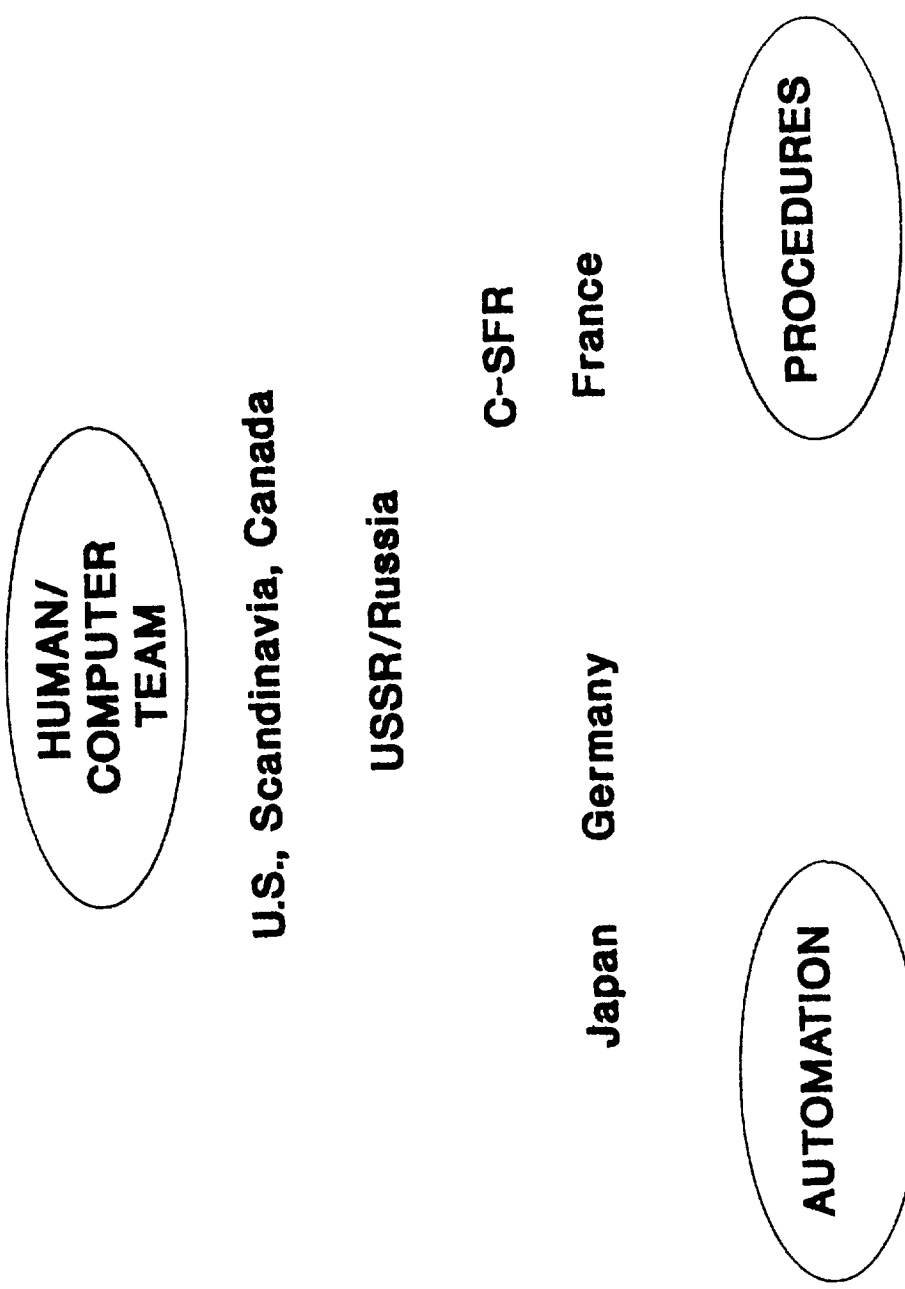


Figure 2.4. Definition of the Operator's Role in Control Room Design of the Countries Studied

REFERENCES

1. Hansen, K. F., E. A. Evans, W. B. Behnke, D. R. Olander, S. B. Cousin, J. D. White, and V. H. Ransom. *JTEC Panel Report on Nuclear Power in Japan.* NTIS no. BB90-215724. Springfield, VA:National Technical Information Service, 1990.

2. Reason, J. T. *Human Error.* New York:Cambridge University Press, 1990.

3. Norman, D. A. *The Psychology of Everyday Things.* New York:Basic Books, 1988.

4. Adler, P. "New Technologies, New Skills." *California Management Review* XXIX (no. 1, Fall 1986).

5. Montmayeul, R., A. Lestien, Y. Dien, and J. Bozec. "Two Aspects of the Technical and Ergonomical Evaluation of the Advanced Control Room of the New French PWR Units." Specialists' Meeting on the Human Factor Information Feedback in Nuclear Power: Implication of Operating Experience on System, Analysis, Design and Operation, Roskilde, Denmark, 25-27 May 1987.

6. Aleite, W., K.H. Geyer, "Safety Parameter Display System Functions Are Integrated Parts of the KWU KONVOI Process Information System," Fifth International Meeting on Thermal Nuclear Reactor Safety, pp. 723-732, Sept. 1984.

7. Hofmann, H. "Cockpit Concept: Small and Simple." *Nuclear Engineering International* (July, 1989).

8. Felkel, L. "The STAR Concept, Systems to Assist the Operator During Abnormal Events." *Atomkernenergie/Kerntechnik* (Germany) 45 (4):252-260 (December 1984).

9. Sackett, J., P. Planchon, B. Sun, J. G. Williams, J. D. White, L. Beltracchi, B. R. Upadhyaya, and D. D. Woods. *European Nuclear Instrumentation, Control, and Safety Technology.* Washington D.C.:National Science Foundation, 1989.

10. Elzer, P., H. Siebert, and K. Zinser. "New Possibilities for the Presentation of Process Information in Industrial Control." Third IFAC/IFIP/IEA/IFORS Conference, Oulu, Finland, 14-16 June 1988. International Federation of Automatic Control, 1988.

11. Elzer, P., H. W. Borchers, C. Weisang, and K. Zinser. "Knowledge-Supported Generation of Control Room Pictures." In *Proceedings of the IFAC Workshop* (Clyne Castle, Swansea, UK, 21-23 Sept. 1988). International Federation of Automatic Control, 1988.

12. Elzer, P., C. Weisang, and K. Zinser. "Knowledge-Based System Support for Operator Tasks in S&C Environments." *Proceedings of the 1989 International Meeting on Systems, Man, and Cybernetics.* (Boston, 1989).

13. Zinser, K. "Design Issues and Knowledge Representations for Modern Control Room Interfaces." *Proceedings of the IFAC Workshop.* See Ref. 2.10.

14. Woods, D. D., J. A. Wise, and L. F. Hanes. *Evaluation of Safety Parameter Display Concepts.* NP-2239. Electric Power Research Institute, 1982.

15. Gonchukov, P. (of VNIIAES). "Evaluation of Sources of Operator Misfunctions and Mistakes for VVER-1000 NPPs." Paper presented to panel at the Kurchatov Institute, Moscow, December 1990.

16. U.S. Nuclear Regulatory Commission. *Human Factors Evaluation of Control Room Design and Operator Performance at TMI-2.* NUREG/CR-1270. U.S. Nuclear Regulatory Commission, 1981.

17. Rogovin, M. (Dir.) "Three Mile Island, A Report to the Commissioners and to the Public." Nuclear Regulatory Commission Special Inquiry Group, U.S. Nuclear Regulatory Commission, 1981.

18. Haugset, K., O. Berg, J. K. Fordestrommen, and W. R. Nelson. "ISACS-1, The Prototype of an Advanced Control Room." IAEA-SM-315/16, pp 9-13. International Symposium on Balancing Automation and Human Action in Nuclear Power Plants, Munich, July 1990.

OTHER REFERENCES

Bohr, E. "Design of Nuclear Power Plant Control Rooms: Some Findings and Possible Improvements." In *Operational Safety of Nuclear Power Plants, Proceedings of an International Symposium* 1:221-29 (1984).

Chachko, S. A. "Ways of Preventing Errors by the Operating Personnel of Nuclear Power Stations." *Elektr. Stantsii* (U.S.S.R.) no. 3:6-10 (1987).

Frederick, E. R. "Design, Training, Operations--The Critical Links, An Operator's Perspective." IAEA-SM-296/91, pp 21-25. International Symposium on Severe Accidents in Nuclear Power Plants, Sorrento, Italy, March 1988.

Helander, M. (ed.). *Handbook of Human-Computer Interaction.* New York:Elsevier Science Publishing Co., 1988.

Hollnagel, E. and D. D. Woods. "Cognitive Systems Engineering (New Wine in New Bottles)." *International Journal of Man-Machine Studies* 18:583-600 (1983).

Pain, C., G. Guesnier, and J. Guilmin. "The Control Room and the Test Simulator", in *Revue Générale Nucléaire*, an entire issue devoted to "The Command-Control Structure of the Units of the N4 Model" (in French) no. 2 (March-April 1987).

Pew, R. W., D. C. Miller, and C. E. Feeher. *Evaluation of Proposed Control Room Improvements Through Analysis of Critical Operator Decisions.* NP-1982. Electric Power Research Institute, 1981.

Rasmussen, J. *Information Processing and Human-Machine Interaction, An Approach to Cognitive Engineering.* New York:Elsevier Science Pub. Co., 1986.

Reinartz, S. J. and G. Reinartz. "Analysis of Team Behavior During Simulated Nuclear Power Plant Incidents." In *Contemporary Ergonomics 1989,* ed. E. D. Megaw. Proceedings of the Ergonomics Society's Annual Conference, "Ergonomics - Designing Progress," 1989.

Sheridan, T. B. "Understanding Human Error and Aiding Human Diagnostic Behaviour in Nuclear Power Plants." In *Human Detection and Diagnosis of System Failures* (Proceedings of a NATO Symposium), eds. J. Rasmussen and W. B. Rouse, pp 19-35. NATO, 1981.

CHAPTER 3

TRANSITION FROM ANALOG TO DIGITAL TECHNOLOGY: CURRENT STATE OF THE ART IN EUROPE

Lester C. Oakes

INTRODUCTION

When nuclear reactors were being developed in the 1940s, state-of-the-art instrumentation and control (I&C) systems were of the analog type.[1] Analog instruments were at that time being used extensively to enhance industrial processes such as pulp and paper and petrochemical production. Where applicable, analog techniques were applied virtually unchanged to nuclear reactors, especially in the conventional parts of the plant. In the nuclear portion of the plant, different fundamental phenomena were being measured, but nevertheless by analog methods. Analog methods have served the nuclear communities well both in the United States and in other countries.

Soon after power production from nuclear plants began to increase, digital computer technology began to expand.[2] By the 1970s, digital technology had undergone rapid improvement. Reliability, capability, size, and especially cost had improved to the point where digital technology could begin to replace the older analog equipment. The commercial process industry has now largely moved

---

[1]An analog instrument is one in which the variable being monitored, such as pressure or temperature, is continuously transformed into another form, such as current, voltage, or pneumatics. The transformed analog signal can then be manipulated mathematically or used to provide indication of the variable's instantaneous condition, such as amplitude or rate of change.

[2]In digital control technology, the signal also begins as a continuous analog signal. It is then soon converted to some binary form much the same as is done in a compact disc (CD) audio system. While in digital form, the signal is free from the drift encountered in many analog systems and can be manipulated in very sophisticated mathematical equations. Information in digital form may be used directly in man-machine interface applications, or it may be converted back into analog form for use in actuators, indicators, etc.

from analog systems to digital systems. For a number of reasons, the nuclear industries in both the United States and Europe have been slow to move away from the established methodology. This failure to move with the other industries in control technology has left the nuclear industry in many countries without a supporting infrastructure to supply parts and technology improvement for the older systems.

Upgrade Strategies

The nuclear communities in both the United States and Europe are now moving towards a greater use of digital equipment (Refs. 3.1-3.3) as they upgrade their instrumentation and control systems. The transition to digital equipment has been progressing on both a piecemeal basis and through complete change-out of the analog equipment.

Piecemeal change. Piecemeal upgrades have been made when problems with analog components have occurred; replacement has been made with digital components having identical functionality. (This method has been employed in the United States and the Soviet Union.) The piecemeal approach has the following advantages:

1. Improved component reliability
2. Replacement parts are available
3. The operator interface remains unchanged

The major disadvantages of the piecemeal approach are as follows:

1. Functionality is limited to that designed to meet the original requirements of the analog equipment; the method does not permit utilizing the extended capability of modern digital systems.
2. It retains the man-machine interface familiar to present operators, but loses the advantages of future technology moving toward more compact control rooms that present synthesized data to operators, allowing them to better coordinate overall control strategies.

Piecemeal upgrades will likely result in a control room man-machine interface (MMI) lying somewhere between the older and the newer, compact versions.

Complete change-out. Total replacement of older equipment with modern digital systems is the other option for designers to consider (Ref. 3.4). This is the strategy preferred by the French for upgrading their older 900 and 1300 MWe

plants with the new N4 reactor control room concept (Refs. 3.5-3.7). Therefore, their retrofit strategy for these plants is to shut them down for a few months while installing the new MMI. During the shutdown, the operators are to be retrained on the new system. The Soviet Union (Ref. 3.8) and the United States are still studying their overall upgrade strategies. However, a number of individual subsystems have already been changed over to digital from analog.

FRENCH UPGRADE RATIONALE

Significant New Digital Systems

Obsolescence is given as the main reason for implementing new hybrid systems in France. (This is, of course, the main reason that U.S. nuclear and fossil plants are considering upgrading their I&C systems.) The second reason given is to be able to harvest the benefits of improved technologies.

The French have made extensive application of digital technology both in upgrading the 900 and 1300 MWe control and protection systems, and in the new design of the N4 1500 MWe reactor concept (Ref. 3.9). The N4 control system is the P20 developed by CEGELEC. The core protection and control system is the C03 developed by Merlin-Gerin in collaboration with Framatome and Électricité de France (EDF). The C03 consists of three main systems: the integrated digital protection system, SPIN; the neutron instrumentation system, RPN; and the regulating rod system, RGL. (The architectures of these control and protection systems are discussed in other sections of this report.)

The French rationale for leaning more heavily toward digital technology as opposed to analog in the above hybrid systems is that digital technology offers a large number of both generic and specific systems improvements.

Generic Improvements From Digital I&C Systems

1. More sophisticated control capabilities. These are provided through improved calculation of nonlinear algorithms and automatic variable weighting to meet different operating modes and conditions; the ability to combine functional units such as signal conditioning and logic units in a single module expedites wiring and ensures more efficient control.

2. Lower cost. Advanced digital techniques coupled with local area networking are economical because they require less space and have less cabling. They also permit incorporating future changes at low cost.

3. Improved accuracy. Calculations made with digital systems are more accurate than analog calculations. This is true because the larger number of analog modules required to perform more complex functions incur accumulated errors that contribute to larger overall inaccuracy.

4. Improved operating margins. Settings remain stable over long periods of time, and inherent noise and drift are reduced: these features permit the setting of better operating margins, as do more complex plant protection system algorithms.

5. Ease of operation. Digital technology makes operating and maintenance actions easier to perform, resulting in less risk of errors.

6. Broader information and data handling capabilities. Distribution of plant data on buses makes information available for a variety of uses as required for plant operation, diagnostics, and maintenance information.

7. Long-term availability of parts and service. Unlike analog equipment, which is usually application-specific, digital equipment can be adapted to a variety of functional requirements. Therefore, digital system performance specifications can be prepared that make it unlikely that spare parts will become unavailable in the near future.

Specific Systems Improvements From Digital I&C Systems (1300 MWe Plants)

Steam Generator Level Control

1. More sophisticated control capability.

2. Ease of reconfiguration. A remote loading facility is used to reconfigure control functions and to program new control strategies during start-up or if modifications are decided at a later date.

3. Accurate, drift-free parameter settings that do not require periodic recalibration.

4. Failure detection capability that provides a selection of automatic corrective actions following module failure.

5. No requirement for a switch-over mode between the high-load and low-load control modes, since both main and bypass feedwater valves can have the same controller.

6. Transition to measured steam flow can be done when the system determines that measured flow is sufficiently accurate (with old analog systems, switch-over from estimated to measured steam flow was done simultaneously with changeover from low load to high load).

Pressurizer Level Control

Because the pressurizer charging nozzle is an area subject to high wear, it is desirable to reduce temperature fluctuations in the charging line. By using a more complex algorithm based on hot-leg/cold-leg differential temperatures, the temperature fluctuations at the charging nozzle have been reduced from 15°C to 5°C during frequency control operation.

Boron Concentration Control

Responding to load changes or frequency changes requires considerable operator skill when done manually. This is due to the disturbance in axial power distribution caused by changes in rod position and boron concentration required by the transient. A digital system has been implemented in one 900 MW unit using the following system considerations: boron addition and dilution time response, system fluctuations, and response optimization.

GERMAN UPGRADE RATIONALE

Limited Use of Digital Systems

In Germany, the rationale for using digital computers also has an accompanying rationale for not using digital computers. The German designers have been using digital computers for certain process functions since 1968 (Refs. 3.1, 3.10). At the time, the computer was used to calculate power density in the core and percent burnup from a system of metal balls called the Aeroball System, in which metal balls are inserted in the core for a period of time, then removed and measured for induced radioactivity (Ref. 3.11). This system was followed by the application of a twin computer system to predict, by performing multidimensional simulations, optimum control rod manipulation strategies (Ref. 3.1). Computers used in the German pressurized water reactors (PWRs) can calculate three-dimensional power densities from aeroballs in about ten minutes. In boiling water reactors (BWRs), the computers can calculate whole-core power density using travelling in-core probes in about three hours.

Other than in the above applications, very little additional application of digital technology has been made in the German system. Upgrading of the German

reactor protection systems by Siemens/Kraftwerk Union has been done with analog technology. The system, called EDM (Ref. 3.12), is similar to the British LADIC system in that it utilizes pulsed saturable reactor technology in a 2/3 coincidence scheme. The first application of an EDM-system was in the Obrigheim NPP (1969) and a modified, enhanced version at the NPP Philippsburg II since 1984.

In the United States and France, one of the motivations for switching from analog systems to digital systems is the unavailability of replacement components for obsolete equipment; in Germany, however, there appears to be sufficient demand for analog equipment to support a supply and technology industry. Thus, the move in Germany toward digital technology is driven by other considerations.

The Germans plan more extensive use of digital technology in the future (Refs. 3.2, 3.3). Their rationale for moving to digital technology for both nuclear and fossil plants is embodied in the set of technical and policy goals outlined below. With some reservations, the Germans expect that digital systems can achieve these goals.

Technical Goals for Digital I&C Systems

1. Maintain or improve level of safety.

2. Improve plant operation through increased automation and better decision aids to the operator during both normal and reset conditions.

3. Utilize standard digital hardware to the fullest extent to increase system reliability, minimize training problems for maintenance personnel, and insure cost-effectiveness (some of the panel's hosts in Germany said if standard commercial hardware is not adequate, upgrading with digital equipment is not feasible).

4. Permit the development of smart sensors and actuators.

5. Support licensing procedures.

Policy Goals for Digital I&C Systems

1. Must be applicable to all new plants.

2. Must be capable of being backfitted to old plants.

3. Must be capable of shortening qualification period for new reactors.

4. Should reduce plant cost and space requirements.

Reservations About Digital I&C Systems

The Germans have set forth some of their reasons for not proceeding too rapidly toward digital technology:

1. The increased information density in a single device greatly increases the consequences of a failure.

2. Cycle times of serial processors cause greater reaction times than for analog devices.

3. Local area networks cause problems.

4. Equipment environmental requirements are more severe.

5. Data storage and retrieval requirements are of a large scale.

6. Mixing equipment from different vendors is difficult.

7. There is a greater potential for failure propagation.

Other Considerations for System Upgrades

Goals for overall digital or analog system reliability are in the range 10^{-3} to 10^{-4}. The Germans believe human operators have adequate reliability for long-time response (minutes) but not for rapid response (seconds); hence the emphasis on more complete automation.

The German designers have emphasized simplicity in the design of their instrumentation and control systems. However, the limitation system (Ref. 3.1) is by nature somewhat complicated and is a likely candidate for utilizing more digital technology.

One of the major advantages the Germans claim for digital systems is that of obtaining diversity by augmenting directly measured variables with an equivalent parameter obtained by computing it from other variables.

The German staff at Gesellschaft fur Reaktorsicherheit (GRS) are interested in developing standards for application to either digital or analog systems, e.g., specifications that describe overall system requirements. An interesting idea put forth by the GRS staff was the possibility of developing generic or universal software that could be used in either a digital or analog application (Ref. 3.13).

FRENCH UPGRADE IMPLEMENTATION

The French are moving toward both partial and complete upgrades of their 900 MWe and 1300 MWe units and toward developing new technology for the N4 1500 MWe plant.

Control System Upgrades[3]

Partial upgrades--1300 MWe plants. Several manufacturers market suitable modular hardware, but Framatome chose CEGELEC's Micro-Z equipment. Twelve units of the French 1300 MWe units have been equipped since successful application to Cattenom 1 in 1986. The system consists of a number of self-sufficient cards, each including the following:

1. Up to 24 logic inputs
2. Up to 8 analog inputs
3. Up to 4 outputs for auto/manual stations
4. One microprocessor for calculations
5. One microprocessor for data and communication management
6. Bank of random access memories (RAMs) for storing time-dependent variables
7. Bank of erasable programmable read only memories (EPROMs) for storing the operating system. The EPROMs contain the algorithm library logic functions, thresholds, filters, etc.
8. Bank of electrically erasable programmable read only memories EEPROM storing the user's program and the settings.

As an example of an equipment requirement, implementing a steam generator level control system requires a total of three cards per steam generator.

Complete upgrades. The French say a complete upgrade can be achieved by using as many Micro-Z cards as necessary. However, a lower-cost system with improved reliability and operability is available with the P-20 Controbloc equipment

[3]For a general discussion of system upgrading in France, see Ref. 3.14.

manufactured by CEGELEC. This control equipment was chosen for the new 1500 MWe reactors. Some of the main features of the P-20 system are:

1. Use of 16- and 32-bit microprocessors

2. Fault detection capability

3. Redundant functionality

4. Use of high-level programming languages such as C

5. Extensive algorithm library with thorough software verification

6. Can be interfaced with both existing and more modern equipment

Protection System Upgrades

Older 900 MWe plants employed a safety system based on a function of coolant channel t's or Delta-T. Development of a new protection system was started in 1976. It was based on functions of the departure-from-nucleate-boiling ratio (DNBR) and the linear power density in the core. This complex three-dimensional algorithm was made possible by the incorporation of digital computers in the system and the successful development of a 6-section ex-core detector, a calculated radial peaking factor, and control rod position to calculate DNBR to the required accuracy.

Both the axial power distribution algorithm and 6-section detectors were tested successfully in the Bugey 2 plant in 1979-80. The DNBR algorithm was then tested successfully at Tricastin 3 in baseload operation and load following operation. In 1984, the new system was installed and tested during the power ascension tests at Paluel 1 and 2 (1300 MWe units). The French safety authorities have approved the use of digital technology in safety systems, subject to two conditions:

1. A software quality assurance program is implemented.

2. The safety philosophy includes the condition that any postulated accident is detected by at least two different functions (functional redundancy).

The U.S. Nuclear Regulatory Commission (NRC) has studied the Paluel experiments and concluded that the French system was as satisfactory as that used in U.S. reactors. Framatome has proposed that a 5 percent improvement in operating margins could be obtained by retrofitting the 900 MWe plants with the same modern protective functions as those used in the 1300 MWe plants.

The digital central processing unit utilizes a Motorola 8-bit microprocessor.

Advantages claimed for the system over the previous t system include improved safety and operating margins, better power maneuverability, and better fuel management. This system had been installed in all 1300 MWe units in France (20 units). Retaining the same architecture and taking benefit from the operating experience of 1300 MW units, an upgraded equipment has been developed. It is installed in 1500 MWe units (3 under construction) and incorporates modern technologies such as 16 bit Motorola microprocessors, local area networks, fiver optics, and programmation using high level languages.

SPIN system. The SPIN protection system (Ref. 3.6) was developed during the 1980-84 time frame. It was installed in 20 sites over a seven-year period, 1984-89. Lessons learned are being applied to the new version in the N4 1500 MWe reactor. Development of the new N4 system is nearly complete (a complete configuration is undergoing tests). The basic difference between SPIN-P4, the 1300 MWe version, and the SPIN-N4 is the incorporation of diagnostic units, 16 bit processors and extensive local area networks (LANs).

Software Verification[4]

Verification of the French 1300 MWe protection system software was conducted by Merlin Gerin, manufacturer of the equipment. The development has 8 stages:

1. Software specification
2. Preliminary software design
3. Detailed software design
4. Coding
5. Tests of individual subroutines
6. Tests of the integrated system
7. Validation tests
8. Interconnected tests

[4]For a discussion of software verification, see Refs. 3.6 and 3.15.

The tests consist of imposing test vectors into the input and then verifying that the outputs behave predictably. Merlin Gerin safety critical software development involves extensive effort in verification. As a rule, the time allocated to verify and validate the software is 70 percent of the time spent to specify, design and code. Its software development requires approximately one hour per line of code. Merlin Gerin uses fault avoidance in writing code but believes that striving for zero faults is an unachievable goal.

In implementing its digital control and protection systems for the 1500 MW NPP, the Merlin Gerin group has developed an interactive graphic tool called Specification of Applications and Automated Generation (SAGA) to cover the design, programming documentation, and administration phases of the software life cycle (Ref. 3.6). SAGA is an attempt to reduce errors between the system specifications and its implementation. Functionally, it automatically generates code while also producing documentation. It is written as a data flow language.

The University of Grenoble has an automatic programming language, LUSTRE, that converts the SAGA text to classical Boolean logic. It is then possible to verify that the Boolean properties are invariant, i.e., to proof that the system cannot give an unsafe output. Those at the University of Grenoble believe this test is more useful than the classical approach of converting to Laplacian operators and applying classical mathematical methods. Their contention is that the fundamental problem with the classical method is that it does not include some important aspects of the software such as the validity of the input specifications. The Boolean approach avoids the problem.

Code Simplification

The code development group at Merlin Gerin believes that excessive complexity is the greatest detriment to obtaining high-quality codes. It has attempted to reduce the complexity of each software module by means other than dividing it into two or more less-complex modules; such division of modules leads to other problems that result in even less overall reliability.

To assess complexity, a special method has been developed in which complexity is analyzed by a tool called LOGISCOPE. Several module components that have quantifiable complexity have been identified. Examples are number of variables, number of loops, and number of blocks. Each of these components has been assigned vector space about a circle, directed away from the center as spokes in a wheel. Each component is examined and the complexity is assigned a number that is then represented as the length of that particular space vector. When the complexities of all components are represented by their length on the vector diagram, an effort is made to circumscribe a circle representing the maximum allowable complexity of the module about the vectors such that none of them

extend outside the circle (see Fig. 3.1). If some fall outside the circle, the author of the software module is asked to attempt to simplify it. If all efforts at simplification fail, the module may be approved for use but marked with a special tag that identifies it as an item to be scrutinized more carefully.

Having gone through the simplification process defined above, the choice of using analog or digital hardware is the designer's. However, the French say that both their commercial and military data show that digital hardware is more reliable than analog.

Digital Application to Experimental Reactors

The French have developed a nuclear instrumentation system for application in the EOLE and MINÊRVE experimental reactors (Ref. 3.16). The system is called SIREX. SIREX has three isolated channels of nuclear instrumentation. Each channel consists of one low-level count rate circuit and one high-level compensated ionization chamber channel. The detectors go through one level of analog signal conditioning before being converted to digital form for use in the 16-bit microprocessor.

Software verification is given considerable attention in SIREX. It goes through the usual steps of specification writing, preliminary design, detailed design, coding, and testing. An independent team is responsible for developing and implementing test and verification procedures. The standards used for implementation of the hardware system are the same as those used for the N4 reactor controls. Overall response time is 50 milliseconds.

GERMAN UPGRADE IMPLEMENTATION

Control and Protection Systems

As previously mentioned, improved versions of German analog systems are being made as needed. No specific schedules have been established for introducing the first digital system upgrade, but digital systems are now being developed. To accommodate a gradual transition to digital, the Grafenrheinfeld plant has been built in modular fashion. By this method small, well-defined increments of the plant can be converted with minimum disruption of the plant.

The digital system now being developed is the BELT-D (Refs. 3.3, 3.17, 3.18). Both the operational and safety I&C systems included in BELT-D have redundant channels of information. Signals are used in both the safety and operational channels, with the safety system having first priority. The BELT-D has five levels of architecture. The architecture of Germany's proposed digital system will be

covered in more detail elsewhere in this report. Briefly, the system consists of four independent channels of safety working into dual isolated data busses. The digital control is carried out by dual channels of process data on a common ring bus (Ref. 3.17).

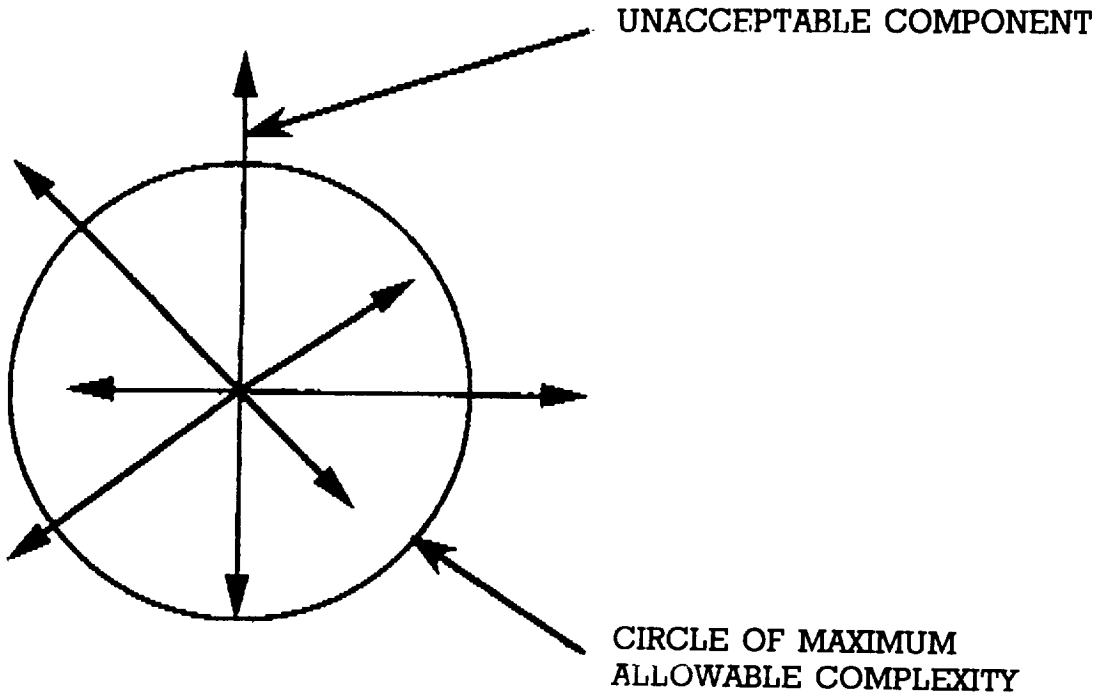


Fig. 3.1. Complexity Paradigm

German designers have identified three levels of safety tasks, S1, S2, and S3 (Ref. 3.19), defining different levels of action to deal with varying levels of severity of challenges to the safety system. By this strategy, the most extensive software verification and validation will be applied to the most critical safety functions, the S1 levels. Less stringent techniques will be applied to the levels of lower importance. The designers have also identified two levels of reliability of control actions, B1 and B2. B2 is for normal process functions, while B1 is for higher reliability requirements such as control of safety variables and critical diagnostic tasks.

Software Development and Verification

Software and verification methods have been developed for the German digital I&C systems. A tool called Specification and Coding Environment (SPACE) (Ref. 3.18) for deriving formal system specifications has been developed using computer-aided engineering (CAE). Specifications developed by the reactor designer are converted to functional diagrams that can be used with any hardware system. During verification and validation, the functional requirements, reliability requirements, and performance requirements are converted into a formal system specification. Codes are first tested using a plant dynamic simulator. Performance is confirmed by proper dynamic response of the plant. A complete safety system is then built using the resulting software. This permits the testing of response time, for noise problems, and for correctness under a range of situations. These tests are to be carried on for about three years.

COMPARISON OF EUROPEAN & U.S. STATE-OF-THE-ART DIGITAL SYSTEMS

Components for making the transition to digital in the United States are well ahead of those in Europe. Most of the complex components such as microprocessor chips used in Europe are all bought from the United States--for example, the Motorola 68000 is widely used. Also, many of the computers are manufactured in the United States. There are numerous examples of European installations using Digital Equipment Corporation (DEC) and International Business Machines (IBM) hardware.

However, digital technology in nuclear power plant control and instrumentation systems is being much more widely applied in some European countries than in the United States. France has developed the world's most advanced control room for the N4 reactor. (Canada and Japan are also ahead of the United States in application of digital systems to nuclear power plants.)

The research and development work that has been done in Europe has required a large amount of money and manpower. Much of the work has been directed toward establishing the fundamental requirements of digital systems as applied to the control and protection of nuclear reactors. Although the environments are quite different in Europe and the United States, the European work that has been done will provide a technical foundation from which the United States can begin its transition to digital when the time is appropriate.

This is so because much of the development has been of a generic nature. For example, all of the European countries are stressing the need for standardization of hardware and data highway networking systems to reduce the impact of

equipment obsolescence; also, many important reliability issues have been addressed. This point is particularly appropriate in software quality assurance for sensitive systems. In this latter area, the French have heightened U.S. awareness of important factors affecting ultimate software reliability such as algorithm complexity.

In the transition from analog to digital I&C equipment, it would appear that the nations of this study could be ranked as follows: France, Canada, United States, Germany, Soviet Union, and Czechoslovakia.

REFERENCES

1. Aleite, W. "Computer Applications For Nuclear Power Plant Operation and Control in the FRG." ANS Topical Meeting, Pasco, WA, 8-12 Sept. 1983.

2. Hoffman, H., H. D. Fischer, K-H. Lochner, U. Mertens. "Microprocessor-based Information and Control Systems for Safety and Non-Safety Applications in Nuclear Power Plants of the Nineties." European Nuclear Conference, Lyon, France 23-28 Sept. 1990.

3. Hoffman, H., H. D. Fischer, K-H. Lochner, U. Mertens. "Digital Information and Control Systems for Safety and Non-Safety Applications." European Nuclear Conference, Lyon, France, 23-28 Sept. 1990.

4. Raimondo, E. "Instrumentation and Control Revamping." International Conference on Operability of Nuclear Systems in Normal and Adverse Environments, Lyon, France, 18-22 Sept. 1989.

5. Guesnier, M. G. "An Entirely Computerized Control Room for the N4 PWR." *Nuclear Engineering International* 32 (no. 394, May 1987).

6. Pilaud, E. "Development and Qualification of Core Protection and Control System CO3 For N4 Type Reactors." Copy of presentation given by Mr. Pilaud.

7. Aschenbrenner, J. F., J. M. Colling, and E. Raimondo. "Reactor Instrumentation and Control For the French N4 Nuclear Power Plants Units." IAEA-Microprocessors in Systems Important to the Safety of Nuclear Power Plants, London, 10-12 May 1988.

8. Personal communication with Soviet spokesman at the JTEC Workshop, Washington, DC., 31 Jan. 1991.

9. Guesnier, G., M. Anglaret, J. M. Collings, and E. Raimondo. "Control and Instrumentation Systems for France's N4 NPPs." *Nuclear Europe* 9 (no. 1, Sept. 1989.

10. Aleite, W. "PRISCA: KWU's New NPP Process Information System." *Nuclear Europe* Vol. 3, pp.24-26 (Oct. 1989).

11. Endrizzi, I. and C. Wenndorff. "PDD and Aeroball Improve Flexibility." *Nuclear Engineering International* 34 (no. 435, Dec. 1989).

12. Kiessler, F. J., K. Hellmerich, and W. Schramm. "Modernizing Reactor Protection." *Nuclear Engineering* 34 (1989).

13. Personal Communication with Dr. W. Bastl, 30 Nov. 1990.

14. Tetreau, F. and A. Parry. "Instrumentation and Control Revamping." Framatome Nuclear Products and Services Technical Bulletin.

15. Bergerand, J.L. "A Global Approach For Software Design In A Dependable Context." International Working Group, Nuclear Power Plant Control and Instrumentation, Lyon, France, April 1990.

16. Burel, J.P. and C. Ringeard. "A New Design For Experimental Reactor's Digital Nuclear Instrumentation System." Specialists Meeting on Microprocessors in Systems Important to Safety of Nuclear Power Plants, London, 10-21 May 1988.

17. Hofmann, H. M., M. Jung, and N. Konig. "BELT-D Offers Plant-Wide Integration of Digital I&C." *Nuclear Engineering Int.* 34 (no. 425, Dec. 1989).

18. Personal Communication with Dr. A. Graf, KWU, 29 Nov. 1990.

19. Druschel, R., W. Maier, and W. Schramm. "Modernization of I&C Systems in Nuclear Power Plants." European Nuclear Conference, Lyon, France, 23-28 Sept. 1990.

CHAPTER 4

COMPUTERIZED OPERATOR SUPPORT SYSTEMS FOR FAULT MANAGEMENT

A. L. Sudduth

INTRODUCTION

The use of nuclear technology for power generation presents unique challenges to power station operators. These challenges include the complexity of equipment and processes, the potential economic and environmental consequences of malfunctions, and the need to increase reliability and quality of operation in order to reduce the cost of electricity from nuclear facilities. The complexity associated with monitoring and controlling a nuclear station is characterized by centralized control rooms with hundreds of annunciator alarms and thousands of individual process measurements. Even during normal operation, the operator must survey and interpret very large amounts of data and draw appropriate conclusions concerning the state of the many systems. In an abnormal or accident situation, information conveyed to the operator may increase beyond timely comprehension. There is a recognized need in the industry for tools that enhance the operator's cognitive ability with respect to understanding the status of plant processes and formulating appropriate strategies to cope with abnormal conditions.

This chapter uses the general term *fault management* for the series of actions that must be taken in a nuclear power plant in response to an abnormal or upset condition. Because nuclear stations are provided with automatic protective systems that are designed to prevent serious consequences for many possible faulted conditions, the problem of fault management in nuclear plants may be viewed as a combination of automatic actions by engineered systems and actions

by the human operator. The human operator, however, has the ultimate responsibility for safety of the plant and the continuity of its power production mission; therefore, this chapter will concentrate on how the instrumentation and control systems in the plant assist the human operator in accomplishing this responsibility.

With the integration of computers into the gathering and storage of data from plant measurements, there is an opportunity to increase the effective use of measurement information by operators, particularly under upset conditions when the amount of relevant measurement information increases significantly. By creating a partnership of human and machine and dividing the responsibility for operation between the human operator and the automatic control system in appropriate ways, the ability of the operator to assess measurement data and to take timely and correct actions can be improved, and the operator can become a more effective fault manager. This survey is concerned principally with the methods by which the Europeans have begun to incorporate more sophisticated and innovative computer based technologies to support the operator in the role of fault manager.

Background: Disturbance Analysis Research

Research in the United States and Europe in the early 1980s considered the problem of what was then called disturbance analysis. This work should be considered the forerunner of the efforts at formalizing the fault management problem today. In disturbance analysis, any deviation of the plant from its expected behavior was defined as a disturbance. It was recognized that disturbances could be the precursors of serious events in the plant, and that it was therefore necessary that the operator recognize and respond to disturbances in an effective manner. Disturbance analysis consisted of a set of methodologies for recognizing, assessing, and mitigating the effects of disturbances in plant operation.

US specifications for disturbance analysis software. The Electric Power Research Institute (EPRI) sponsored research into disturbance analysis that resulted in the development of a specification and a prototype for a Disturbance Analysis and Surveillance System (DASS) that would assist the operator to respond properly to disturbances (Ref. 4.1 and 4.2). The DASS would have the following responsibilities during abnormal plant transients:

1. *Signal validation.* In this function, the system would attempt to determine whether data being gathered from the system sensors adequately represented the values of the measured states. Basic actions would include elimination of channels in test, channels operating outside of the valid calibration range, and indications not consistent with operating mode.

2. *Determination of operating mode.* From a set of six major modes and sixteen submodes of a nuclear station, the current mode of the plant and any appropriate submode would be identified by pattern matching.

3. *Display of plant status.* This display would allow the operator to organize the vast array of information received from the disturbance analysis system. The research established that the effectiveness of DASS would be heavily dependent on an effective graphical user interface.

4. *Configuration verification.* This function would determine whether the current alignment and operability status of plant equipment was consistent with the regulatory requirements for the current mode, in accordance with the station Technical Specifications.

5. *Verification of automatic actions.* This function would trace the progress of various automatic control and protective functions to ensure that they were operating correctly. The operator would thus be relieved of the burden of ensuring that routine control actions actually take place as required.

6. *Determination of margin to limiting conditions.* This function would monitor the system states and compare them with preimposed limits, calculating a margin to exceeding a limit. If a limit was exceeded, then time and extent of violation would be noted. The limits would be based on those contained in the station Technical Specifications.

7. *Monitoring of critical functions.* The disturbance analysis system would determine the operability of system functions critical to the safe and reliable operation of the process, notifying the operator of the impending violation of the objectives of these critical functions.

8. *Alarm-based system fault detection.* Using a symptom based logic for fault detection based only on patterns of alarms, the system would detect the presence of faults.

9. *Parameter-based system fault detection.* This function would provide fault detection based on the values of measured states not in an alarm condition, using parameter estimation.

10. *System fault diagnostics.* This function would attempt to identify the root cause of a disturbance. This function was considered of secondary importance to providing assistance to the operator in mitigation of disturbances and returning the system to a safe, stable condition. It was

based on the concept that diagnosis of the cause of a fault is secondary to ensuring that the system equipment and humans are protected from adverse effects of the fault.

11. *Determination of mitigating action.* This function would provide advice to the operator on the best corrective action once a disturbance had been identified. It was expected that operator response based on symptoms alone, without an intervening attempt to diagnose the situation, would result in proper operator action in a more timely manner.

12. *Monitoring of operator intervention using preestablished procedures.* This function would track the action of the operator in modifying the state of the process.

13. *Prediction of disturbance propagation.* This function would provide information to the operator on the expected future manifestations of a current disturbance. It was expected by the researchers that this function would be nearly impossible to implement using then-existing simulation technology, due to the complexity of the underlying models required.

14. *Assessment of the future effects of current control actions.* This function would provide the operator with a tool to determine the impact of contemplated system interventions.

In the panel's review of nuclear I&C systems and the computerized operator aids that have been developed in Europe, it is interesting to note that many of the requirements of the DASS have begun to be embodied in software systems currently being deployed there. Ideas that were developed and formalized in the United States ten years ago for approaching the problem of making the operator and computerized monitoring system effective partners in fault management have begun to be realized in European nuclear research and in plant applications. In that respect, the panel finds that the Europeans appear to be ahead of the United States in the development and application of advanced computer-based operator aids, particularly those associated with fault management in nuclear stations.

OVERVIEW OF FAULT MANAGEMENT ISSUES

When an unanticipated and unacceptable deviation in system performance occurs, it is classified as a fault. A fault is an excursion in the values of system states in which there is sufficient deterioration in performance or quality to require some attention by the operator or the supervisory system. The urgency of the response depends on the nature of the fault. Certain faults require immediate action due to

imminent danger to the public or to the plant owners' investment; others represent inconveniences that cost money but do not have such dire consequences that immediate attention is required. System faults may be broadly classified into three groups according to the part of the system in which the fault originates: faults caused by changes in system parameters or structure; faults caused by changes or inadequacies in control algorithms; and faults caused by failures in the measurement system. It is the responsibility of the plant monitoring and control systems, acting either automatically or in partnership with human operators, to provide appropriate response to faults. The ability of the operator or of the supervisory control system to provide proper response depends on rapid recognition of the nature of the situation and the formulation and execution of appropriate actions.

Five Components of Fault Management

1. *Fault detection*--determining that a fault condition exists; that system states are no longer within allowable limits. The job of fault detection is made more difficult because a plant may undergo an expected transient, such as a load change, which may cause symptoms similar to those of a fault. The fault detection function may also be misled by measurement failures.

2. *Fault diagnosis*--localizing a fault and identifying its cause. Localization is difficult because the actions of automatic control systems may propagate the effects of a fault across a number of plant subsystems.

3. *Fault evaluation*--determining the proper action to take in the event of the fault. This implies the presence of some form of fault classification system that maps identified faults into a set of responses appropriate to the type and level of severity of the fault.

4. *Fault mitigation*--taking an appropriate set of actions to counteract the effects of the fault on the plant, at least to the extent that the plant remains in a safe condition and damage to equipment is minimized or prevented.

5. *Fault management success assurance*--ensuring that the action taken has been effective in response to the fault, and that critical functions associated with plant safety enable adequate thermal margin to be maintained.

The Need for Computerized Fault Management Assistance

The need for computer-based systems to assist the operator in tasks associated with proper management of system faults has been studied extensively. Without specific attention in the design of computerized monitoring systems, the operator is besieged by information from the computer during a typical system fault, and by new information that becomes available before the last set of readings can be discerned and analyzed. This information overload, the so-called "Christmas tree effect" in the control room, creates sufficient confusion that specific diagnoses may be delayed significantly, and the operator is reduced to responding to fault symptoms in an unorganized manner without a clear fault mitigative strategy. This condition, which is commonly referred to as cognitive overload, is caused by the lack of sufficient time for the operator to consider all possible causes of a particular set of observations, to evaluate the consequences of proposed courses of action, and to execute the needed action. Studies of nuclear operator actions in casualty situations demonstrate that this time stress is the most important factor affecting the ability of the operator to respond effectively (Ref. 4.3).

The panel saw in Europe a significant effort to develop the computer to be an aid to operators in time-stressed situations, relieving them of cognitive loads that were not required for proper response, providing automatic response where feasible, and supporting the operator in the task of fault management. The next sections will discuss some of the specific computerized operator support systems that have been developed by European researchers and that certain operators of European power stations are using to advantage in fault management. These systems will be discussed in categories according to the specific fault management task for which they are intended. An effort has been made to show as complete a picture as possible of the fault management systems under development or in use at the places that the panelists visited in Europe; however, the amount of specific technical information concerning each system is limited to a high-level functional description. More technical details may be obtained from the research organizations identified in the discussion.

FAULT DETECTION

Deficiencies of Conventional Process Alarm Systems

Monitoring and supervisory systems in U.S. nuclear power stations attempt to assist the operator to perform the function of fault detection through alarms. Actions for the operator to take in response are prescribed in the form of alarm response procedures, usually a set of written procedures contained in a manual in the

control room. Problems in using conventional alarm systems as the primary means of fault detection have been well documented. These include the following:

> Large numbers of alarms tend to reduce the ability of the operator to locate relevant information.
>
> Multiple alarms initiate during any significant transient, so that important indications of abnormal conditions are masked by many less important alarms.
>
> Alarms occur frequently that are irrelevant to the current mode of operation or are created by a specific operator action, rather than occurring as a precursor to the need for operator action.
>
> Alarms remain activated for long periods of time while the associated components are out of service or under repair, so that a number of channels are in the alarm condition regardless of the plant operating state.

The most serious problems with conventional alarm systems as fault detection and diagnosis tools are related to the precedence and timeliness of alarms. Alarms are generally not received in a predictable order during fault situations. Thus the first alarm the operator sees may be a secondary consequence, not a primary indicator of a specific fault. Traditionally, all alarms are equal in precedence, therefore those that are noteworthy because they add new information about a progressing situation are not distinguishable from those that are redundant to previous alarms or are the consequence of an automatic system protective action rather than of the original fault.

In order to prevent spurious alarm actuation during normal plant measurement variations, the tolerance band within which measurements are considered normal has to be made relatively broad, so that expected instrumentation noise and normal variations during process maneuvering do not create false alarms. A significant deviation of system states may occur well before the associated alarms begin to activate.

By the time an alarm has been received, the control system has propagated early system fault response around the various interconnected parts of the system. The actions of the control system in the absence of a plant trip are in many cases to mitigate the system response to the fault, thus obscuring the original fault symptoms. This expansion of the scope and obscuring of the symptoms of faulted system behavior creates diagnostic confusion. As a consequence of dependence on alarms for fault detection, the operator is often notified of an abnormal condition ambiguously and late.

One approach to the problem of how to focus operator attention on the most relevant alarms or other indications of system condition is to segregate a small number of the system indications and associated alarms on a dedicated panel specifically for that purpose. This is the approach taken by the U. S. Nuclear Regulatory Commission (USNRC) in mandating the installation of a Safety Parameter Display System in each nuclear station control room. This static approach to the problem creates a context in which the most relevant indications are available separately from those unlikely to be relevant, but it fails to provide priority within that smaller context, and it does not increase the timeliness of the alarms received. As a result, a significant burden remains on the operator to ensure that measurement data and associated alarms are converted into fault mitigative strategies quickly and correctly.

To a very great extent in the U. S. nuclear power industry today, measurement alarming is the only means provided to the operator for system fault detection, despite advances in computer hardware and software associated with monitoring and controlling modern systems.

New Approaches in Alarm Management Systems

To improve the effectiveness of alarms in conveying useful and unambiguous information to the operator, one approach is to attempt to do some form of alarm prioritization. This has led to the idea that within the set of true alarm signals is a natural hierarchy for any given system condition: alarms that are primary, those that are secondary, and those that are irrelevant. The job of an alarm prioritization system is to establish dynamically where in the hierarchy each alarm belongs.

Knowledge based systems have become candidates for implementing an improved alarm system, although more deterministic approaches have also been implemented, including those based on conventional forms of pattern recognition. The features proposed for knowledge based alarming systems include the following:

> Prioritization of alarm indications in a hierarchy that improves the ability of the operator to determine proper action. This includes suppression of irrelevant alarms, such as those that have no meaning for the current operating mode and those associated with known malfunctions in the monitoring system.
>
> Development of alarm classification schemes that differentiate between alarms that represent the primary indication of a particular condition, alarms that provide confirmatory or secondary indication, and alarms that are unrelated to the primary cause of the alarm.

Presentation of alarms in a manner that promotes correct operator interpretation through the use of human-centered design techniques.

HALO (Norway--Halden Reactor Project). One system that performs these functions in improving alarm system performance is the HALO system developed at the Halden Reactor Project of the Organization for Economic Cooperation and Development (OECD) (Ref. 4.4). Recent refinements to this system, which have been demonstrated in experiments using operators of a research reactor, have shown that operator performance in response to a faulted situation can be improved. It is interesting to note one conclusion of this research is that once a comprehensive computerized process monitoring system has been installed in a plant to monitor the major plant systems associated with power production and plant protection, there is very little reason to continue to use conventional annunciator alarm panels.

Alarm and Status Management System (Germany--Kraftwerk Union and Gesellschaft fur Reaktorsicherheit). In recognition of the alarm management problems posed by significant transients, KWU and GRS developed an alarm management system for the Phillipsburg nuclear station (Ref. 4.5). Alarm suppression is performed by splitting the alarms into functional groups then relating the relevance of each functional group to each of a series of predefined plant transient modes. Alarm sequences are established based on theoretical considerations of alarm propagation, and consequential alarms are suppressed once the primary alarm indications for a particular event have been received.

Electricite de France has no dedicated alarm management system but incorporates alarm management features into the advanced control room designs. These alarm management features reduce the number of alarms created by a transient, perform some alarm validation to eliminate spurious alarms, and allow the operator to take corrective action directly from the graphical alarm screen without the need to refer to written procedures or additional graphics screens.

Though traditional forms of alarm systems will continue to have a place in power station control rooms, particularly for equipment monitoring applications and the benefit of maintenance personnel, the trend is to find more innovative methods for indicating the presence of process faults to the operator.

New Methodologies for Fault Detection

In reviewing European nuclear plants, the panelists noted several systems that have been developed to improve the operator's ability to detect faulted conditions in power plant processes. There are three basic components of the new technology of process fault detection.

1. *More robust methodology to determine the normal or reference values of various process measurements as a function of plant condition.* In traditional alarming systems, these reference values, which may vary over a considerable range during normal plant operation from startup to full load, generally result in the establishment of fixed alarm setpoints relatively far from normal plant measurement values. In the new fault detection schemes that the panel surveyed, the setpoints are dynamic, derived by tracking the plant states using some form of parallel simulation model, thus making fault detection much more sensitive and timely.

2. *Improved methodology for removing ambiguity from the determination that a fault has occurred.* This is done by developing systematic methods for determining when measurements indicate a possible fault by considering the deviation of groups of related measurements as a symptom, rather than the deviation of individual sensor signals.

3. *New methodologies to isolate measurement failures.* Methods for ensuring the quality of measurement information are used so that failures in measurement channels are not mistaken for actual process faults. These methodologies are collectively called *signal validation.*

Robust Determination of Normal or Reference Values of Measurements

One prerequisite for performing fault detection in a process system is the establishment of what constitutes the normal or reference values of a process measurement. In many cases, the normal value of interest will be a constant, in which case a fixed value may be used for comparison with the sensor indication. In many more cases, the value of normal for a particular process measurement varies depending on the operating mode of the process and its operating level or load. In a power station, for example, there are many measurements whose normal values vary depending on whether the plant is operating or shut down, and many whose normal value is directly related to the power output of the station. This situation results in cases where, to perform fault detection, the operator or the operator support system must constantly determine the value of normal based on the situation.

The panel observed that many European organizations have adopted a model-based paradigm for fault detection in which the determination of normal is left to some type of reference model. Figure 4.1 illustrates the reference model paradigm that could be used in fault detection, or in a variety of ways to assist in fault management.

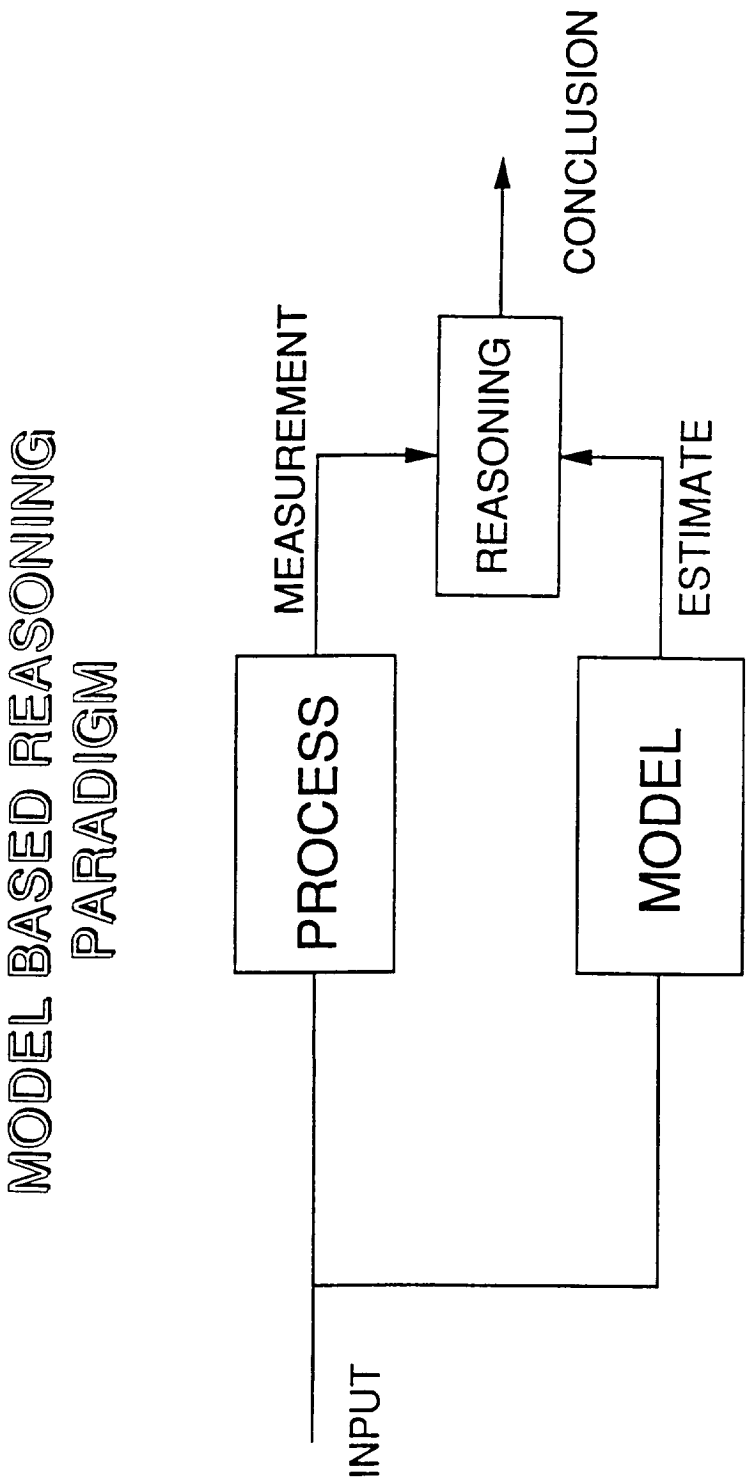


Figure 4.1. Model Based Reasoning

Use of Patterns of Measurement Response in Fault Detection

Process faults rarely result in the deviation of a single measurement. The causal paths within a process tend to propagate failure effects through the process and create multiple sensor deviations. The nature and severity of a process fault may be determined from the pattern of this propagation, and the fact that multiple sensor deviations are noted eliminates measurement failure as a source of the observations.

Use of information from multiple sensors is particularly important when the effects of feedback tend to compensate for the fault. This feedback may arise from the self-regulating nature of many processes or from the action of engineered control systems. If the effect of this feedback is large enough, the effects of the fault may be masked, and sensor deviations may return to normal. The operator may then assume that the condition was an unimportant transient, rather than a potentially serious parameter change.

A model of the process response that incorporates these causal forward and feedback pathways may be used as a basis of removing ambiguity from fault detection, then establish a framework for diagnosis and assessment. Alternatively, patterns of multiple sensor response may be predetermined with simulation and collected in a database with which comparisons may be made. In either case, the use of multiple measurement deviations, considered as a group, provides more robust fault detection capability than single alarms.

Use of Signal Validation in Fault Detection

Measurement signals obtained from process sensors and associated electronic or pneumatic equipment are the only path by which information concerning process status is conveyed to the operator, to the automatic control system, or to a computer-based operator support system. It is therefore very important that the quality of process measurement information be high, and that erroneous information from sensors be quickly and effectively eliminated from consideration by the operator and by any analysis or control functions performed by the process computers. The use of erroneous measurement information in an automatic control function could result in unnecessary process shutdowns or in equipment damage. Analysis of invalid sensor signals by an operator or computer-based system, for example, if an invalid measurement is mistaken for a process fault, may result in misleading or incorrect conclusions and inappropriate responses.

In the typical U. S. control room reflecting the technology of the 1960s, if multiple measurement channels are available for a particular process state, the operator is provided with a manual switch to select which channel is to be displayed or fed

to the control system. If the selected channel fails, the operator moves the switch to the other channel to avoid an adverse impact on the process. With the new technology available for control rooms, a much wider range of options can be employed to improve this situation. This new technology is centered around *signal validation*, a collection of methodologies for ensuring the quality of measurement information.

Signal validation consists of methodologies for distinguishing measurement failures from process faults and selecting which instrumentation signals to use in control and analysis functions. The panel found two methods of signal validation that are used in process monitoring systems in Europe: comparisons among redundant measurements, and the use of reasonableness checking among multiple signals having a quantifiable relationship with the measurement being validated.

Use of Redundant Measurements. Comparison methods are based on the availability of at least two measurements (direct or derived) of a desired process state. These redundant measurements may then be used to make some judgment about the validity of the measurement signals. The simplest comparison methods involve the installation of two sensors at the same location for the same process state. These redundant sensors are automatically compared with each other; disagreement between them larger than a specified threshold (related to the amount of anticipated measurement noise) is considered indicative of failure of one of the measurements; however, more than two measurements are required for an unambiguous measurement quality determination. When at least three measurements are available for comparison, it is possible to make some logical choice of which to accept or reject, and to form a "best estimate" of the true value of the process state.

When there are no physically redundant devices to supply redundant measurement information, it is possible to use analytically redundant measurements. An analytically redundant measurement can be found when there is a process model that can be used to derive a representative value of a directly measured state from measurements of other states. Once three or more representations of a particular measurement are available, there are methods that may be used to discriminate failed measurements and select the most representative "true" value of the measurement.

Use of Reasonableness Checking. The other major method of signal validation is a more qualitative or symptomatic method based on a comparison between the measurement value and certain reference values. These reference values are of two types: estimates of what the measurement should be based on related measurements, and values impossible for a properly functioning instrument to read. If a single measurement has an unexpected value, inconsistent with related

measurements or consistent with known failure modes of the instrument channel, it is likely a measurement failure.

Reasonableness checking may also be performed using information concerning the derivative of a measurement. For most measurement situations, it is possible to estimate the maximum rate of change achievable in a valid measurement, then to apply this estimate as a limit for the allowable rate of change of the channel. This technique is particularly useful for measurement channels with relatively long time constants, such as for temperature detectors in thermowells, or for measurements of process states with long time constants. A common form of applying limits on the derivative is to monitor two redundant measurements, immediately rejecting one whose derivative assumes a high value.

The panel's brief review of signal validation technology in Europe indicates that it is now routinely applied in computerized monitoring systems. It appears that reasonableness checks and other knowledge-based techniques are used more frequently than those based on complex analytical methods. Research into advanced methods of signal validation continue at several locations, including GRS in Germany (Ref. 4.6), but these advanced methods have not yet been deployed in operating plants. GRS has found that analytical redundancy is a very effective method for generating additional measurement information for use in signal validation, but its deployment is inhibited by the lack of process models that can produce the needed analytical results in real time. They are investigating advanced computer hardware devices, such as transputers, to solve this problem.

New European Fault Detection Systems

Early Fault Detection (EFD) System (Norway--OECD Halden Reactor Project). One of the developments in fault detection is the Early Fault Detection system designed at Halden and implemented on the Loviisa power station (Ref. 4.7). In the design of EFD, three important principles are noted:

1. Fault detection consists of determining and assessing the significance of the difference between the values of process measurements and reference values for those measurements that would be considered "normal" in the context of current process operation. It is therefore necessary to determine the definition of "normal" continuously by the use of process models in order that adequate sensitivity may be maintained and false alarms may be avoided as the process load changes.

2. The presence of a fault is indicated by input-output inconsistency within a subprocess, not the absolute value of the subprocess outputs. Fault effects propagate through a process as a result of feedback and

feedforward paths through process structure and the action of automatic controls. One key to localizing and assessing the magnitude of a fault is to locate the subprocess whose output shows faulted behavior while the input is normal.

3. Groups of related measurements, examined together, provide much better fault detection resolution than individual measurements examined singly.

When these ideas are applied in fault detection, as they have been by Halden researchers on their own research simulator and at the Loviisa power station, a very effective fault detection system results. This system has been shown by experience to be much more sensitive in fault detection than conventional alarms or normal operator process monitoring.

Early Fault Detection (Germany--Gesellschaft fur Reaktorsicherheit). Two fault detection systems has been developed by the German nuclear research organization Gesellschaft fur Reaktorsicherheit (GRS) for use in German nuclear stations. The first of these systems derives its basis from disturbance analysis, and is called the Integrated Disturbance Analyzer (Ref. 4.8). This system is designed to notify the operator of the presence of a disturbance as indicated by deviations in plant measurements. The system uses a functional description of the process to develop a set of advanced graphics that are then presented to the operator to enhance the operator's understanding of the plant status. Threats to the continued successful performance of a critical plant function are noted; thus the operator's ability to take timely corrective action is enhanced. This system has been demonstrated on a portion of the Biblis nuclear station.

The second of these systems is based on determination of a number of fault sequences through the use of simulation models (Ref. 4.9). The computer system attempts to match observed behavior with these predetermined sequences that represent faulted behavior. When a close enough match is found, the operator is notified. Likely fault sequences are determined based on the experience of operators and the opinions of expert process designers. This knowledge is then coded into the knowledge base of the fault detection system. This form of early fault detection has been applied at the Phillipsburg nuclear power station.

SINDBAD (France--Centre d'Etudes Nucleaires de Cadarache). In France, research has been performed on early fault detection, resulting in the development of a system called SINDBAD. SINDBAD is an early fault detection system based on a function oriented representation of a nuclear station. The fault detection portion of this system is mainly algorithmic, using reference models against which the operation of the plant is compared. Investigation of knowledge based fault detection systems is continuing using plant simulators, until the cost effectiveness of these systems can be demonstrated.

EXTRA (France--Electricite de France Directiones, Etudes, et Recherches). One possible application of model based fault detection is associated with the action of plant logical controls. Logical controls are responsible for the automation of power stations, and include binary devices such as switches, relays, timers, and programmable logic devices such as overcurrent devices in circuit breakers. The detection of faults in such systems can be based on modeling the logic associated with automation of specific functions, such as the operation of the electrical power distribution system.

One such application, developed by researchers at Electricite de France (EdF), is being applied at the Bugey nuclear power station (Ref. 4.10). This application, called EXTRA, monitors the performance of the extensive power distribution system in the plant, consisting of thousands of separate electrical devices. Based on logical models of how these devices should behave when unfaulted, the system is able to isolate and identify faulted conditions very rapidly.

One interesting aspect of the EXTRA system is that while it is a very large rule-based reasoning system, the rules are generated automatically from structural and functional descriptions of the components and systems of the power station. This makes the software easier to create and maintain than for a system written rule-by-rule using a conventional knowledge-based system development method.

Overall, the fault detection systems that the panel saw in Europe represent significant advances over the use of traditional alarming systems in control rooms. The use of advanced fault detection methods can lead to a significant reduction in plant alarms, allowing stations to achieve "dark board" operating mode under most normal conditions.

FAULT DIAGNOSIS SUPPORT SYSTEMS

Fault diagnosis consists of determining the specific type of failure or event that has created a detected fault. It might be thought of as finding the correct mapping from a single indication or a set of indications to the underlying change in process, control, or measurement system parameter that has caused the failure. The traditional purpose of fault diagnosis is to provide information that can be useful in the formulation of mitigative strategies.

Diagnosis versus Symptom-Based Fault Response

There is ongoing controversy in the United States and Europe about the role of diagnosis in fault management. Because it is common in many situations for mitigative action to be required prior to a complete diagnosis of the nature of the

fault, it has become necessary to develop mitigative strategies that do not depend on diagnosis, but only on the patterns of the symptoms of abnormal process behavior. The action of the operator or supervisory system in this case consists of the performance of mitigative steps associated with preplanned strategies, which are in turn based on maintenance of certain critical functions associated with protection of the system and the environment. The idea of fault response based on symptoms rather than identification of the specific fault event through explicit diagnosis is the basis for much of the recent U. S. work in establishing strategies for mitigating nuclear power station faults.

Where identification of a specific fault event is considered to be important in the planning and execution of mitigation, more information is provided by computer based operator support systems for diagnosis. Diagnostic information then serves to augment the operator's knowledge in formulating and executing mitigation. Where fault response is based primarily on symptoms, not much support may be provided by the computer for the diagnosis step in fault management. In either case, the operator may be provided with a considerable amount of information concerning the severity of the faulted condition, by indication of the amount of deviation of the plant from normal or the closeness of approach of the critical process states to some limiting condition. The need for diagnosis may be delayed by mitigative strategies based mainly on response to symptoms, but the information provided by diagnosis is of critical importance in ensuring the longer term safety of a faulted plant, and therefore cannot be entirely neglected.

In those countries where diagnostic information is considered to be of immediate value to the operator in the planning and execution of fault mitigative strategies, the panel found several organizations that have developed computerized data analysis systems designed to provide diagnostic information. The approach is to use knowledge based systems as a tool for developing diagnostic support systems for the operator.

Use of Knowledge Based Systems in Fault Diagnosis

System knowledge for diagnostic applications may take three forms: structural, behavioral, and functional. These forms have important implications in the development of the knowledge base and the knowledge representation methodology chosen by the diagnostic system developers.

Structural knowledge consists of the physical relationships among the parts of a process, commonly called connectivity, and the manner in which individual system parts are constructed. Knowledge of the structure is important because of the locality property of system faults -- faults affect those parts of the system closest to the fault first. In order to include structural knowledge in the knowledge base,

the diagnostic system must model connectivity among process components and systems.

Behavioral or causal knowledge represents knowledge of how the parts of a system influence each other through connectivity paths. Such knowledge may be described, for example, as a set of differential or difference equations. Through the use of such equations, it is possible to trace a change in a system state to changes in related system states or parameters that represent the possible causes of the change under consideration. The causal relationships are particularly useful in isolating the root cause of an observed system change; in tracing the lowest level system change that produces multiple or sequential manifestations of system failure; and in ensuring that indicated system changes are actual system changes and not instrumentation failures.

Functional knowledge is related to the idea of design intentionality. It is developed from the consideration of why each part of the system was placed there by the designer. Such functional relationships may be necessary for fault diagnosis because certain system failures are caused by deviation from the intention of the designer, rather than a specific component malfunction.

The application of knowledge-based systems to system fault diagnosis of typical nuclear station systems has some unique problems:

> The information upon which the knowledge-based system acts is not a static database, but is being continuously updated. This is because the situation for which reasoning is occurring is itself dynamic.
>
> All of the needed information must be gathered from system instrumentation; there can be no direct inquiry of the operator during a dynamic situation.
>
> Reasoning must proceed in the absence of needed information from unavailable or obviously faulted measurements.
>
> Results must be produced in a timely fashion, that is, soon enough so that an operator taking action on the basis of the results of the diagnostic system can have a significant mitigating effect and minimize economic and safety consequences.

Thus the European systems that successfully address these problems represent very sophisticated applications of knowledge based system technology, and have required substantial investment by the sponsoring organizations. In reviewing of the state of the art in European knowledge based diagnostic systems, the panel

found that deployed systems with the most experience behind them are mainly symptom based reasoning systems, using behavioral knowledge. The main form of knowledge representation used in these symptom based reasoning systems is that of rules.

Examples of Symptom Based Diagnostic Reasoning Systems

DISKET (Norway--OECD Halden Reactor Project). One successful symptom based reasoning system, called DISKET (Ref. 4.11), was developed at Halden in cooperation with the Japanese nuclear research organization JAERI. It is classified as a diagnostic *expert system*, using a knowledge base constructed from characteristics of system transient responses obtained from actual or simulated system faults. The data definition portion of the knowledge base contains the relationships between accident causes and the corresponding system response. Rules in the knowledge base relate system measurements to other measurements (for consistency checking); system measurements to accident hypotheses (for diagnosis); and accident hypotheses to each other. That portion of the system containing rules to relate system measurements to accident hypotheses uses certainty factors in evaluating the likelihood of a particular conclusion. Certainty factors are considered necessary due to the possibility of missing or incomplete data, as from a failed system measurement.

In addition to the normal findings of spatial pattern of events--all conditions satisfied or a portion of conditions satisfied--DISKET contains a temporal reasoning component. This temporal reasoning looks for patterns of the type A AFTER B AFTER C. It increases the power of the diagnosis by recognizing that system response to faults has both spatial and temporal components.

Another interesting feature of DISKET is the use of a hierarchical structure for hypotheses. This use of a hierarchy of accident hypotheses enables the search space to be reduced at an early point in the diagnosis sequence. This is done by eliminating from consideration those hypotheses with very low certainty factors based on a small number of system measurements.

Expert System Based Diagnosis (France--Center d'Etudes Nucleaires de Cadarache). In France, although fault mitigation is to rely as far as possible on symptom-based approaches, work continues on computerized operator support systems for fault identification and localization that incorporate knowledge based techniques (Ref. 4.12). These systems differ in how the tasks of fault diagnosis are shared among algorithmic and logical reasoning. In the SINDBAD system discussed previously, logical reasoning is limited to the processing of high level information produced by function oriented diagnostic modules. By applying logical reasoning at this point, rather than to the measurement data stream directly, the size of the knowledge base is limited to a few hundred rules.

EDES (Soviet Union--All Union Research Institute for Nuclear Power Plant Operations). Another major symptom based diagnostic system, called EDES, was developed at the All Union Research Institute of Nuclear Power Plant Operations (VNIIAES) in the Soviet Union (Ref. 4.13). This system represents the behavior of the process using a set of qualitative semantics. Experts have identified a series of likely fault scenarios and a description of the symptoms of these scenarios using the qualitative descriptive language. Using fuzzy pattern matching techniques, EDES is able to identify and classify faults on the basis of plant measurement information. This system is now deployed in Soviet power stations.

Use of Model Based Intelligent Systems in Fault Diagnosis

An alternative approach to rule based reasoning in fault diagnosis is the use of some form of model based reasoning. The panel found that some successful research has been done in the use of models that integrate structural, behavioral, and functional knowledge, reasoning from physical principles rather than patterns of observations. It is reasonable to conclude that these first principles reasoning systems, because of the greater depth of knowledge contained in them, will ultimately result in the most successful applications. The paradigm of model based reasoning is represented in Figure 4.1, where a model of the process is used as a source of knowledge from which to reason about the observations that are provided by measurement information. Knowledge bases that consist of models can minimize the effort required for knowledge base construction, provide portability from one plant to another and one process to another, permit modularity techniques that minimize the process knowledge required to construct the initial knowledge base, and offer better opportunities for verification and validation. Diagnostic algorithms that analyze models rather than rules can be made more efficient, particularly with respect to the handling of dynamic data, a problem commonly referred to in the artificial intelligence field as *truth maintenance.*

All models are abstractions adopted as tools for studying the world without the complication of perceived irrelevant complexity; however, abstraction introduces error as a consequence of generalization and simplification. The challenge in producing useful models is to apply abstraction judiciously, to account for the limitations in applicability and fidelity, and to recognize unreasonable or nonphysical results when they occur. Models must also be useful in the sense that results are produced that convey sufficient information in a timely manner, so that decision making is improved. These goals certainly apply to models used to represent knowledge of systems and processes for purposes of fault diagnosis.

With increases in computer hardware capability, it might logically be concluded that our striving should be for more and more precise computer representations of physical systems. However, the panel found no examples where the use of a

quantitative model as a predictor of faulted process behavior was used to assist the operator in diagnosis. It appears that quantitative predictions of faulted behavior, when developed from complex dynamic models, may not be useful in assisting humans in assessing system performance. Though the reasons for this may be associated more with presentation and interpretation, humans appear to be overwhelmed by data from quantitative models in the same manner that they may be overwhelmed by data from instruments in faulted situations. Yet, within certain limits, human beings understand and can reason about the behavior of physical processes without requiring detailed numerical analysis. This skill is known to play a major role in disturbance analysis and fault diagnosis by process operators.

Although the mechanisms of human reasoning about physical processes are complex and not well understood, cause-and-effect is clearly a basic mechanism of human reasoning about system behavior. Therefore, systems that reason from effects to causes, using a knowledge base containing principles of process causality as embodied in qualitative models of processes, may be a viable approach for model-based reasoning. The panel found that such systems are beginning to be developed. Two systems in particular were noted in our review as being in the forefront of development of these more sophisticated knowledge based diagnostic systems.

DAIG (Czechoslovakia--Nuclear Research Institute at Rez). In Czechoslovakia, work has begun on a model based diagnostic system called DIAG. The basis of this system is the *influence diagram*, a form of causal knowledge representation previously applied in econometrics and biology. In developing an influence diagram, the analyst attempts to derive behavior from observations of the system response to interesting situations, from whatever scientific knowledge is available concerning the operation of the system, and from knowledge of the system structure, so that causal relationships among the various process measurements and likely process failures may be represented economically.

ALLIANCE (France--Commissariat a l'Energie Atomique). In France, the panel found that CEA, Cadarache, is working on a new diagnostic system called ALLIANCE. This system uses qualitative modeling to represent the structure and behavior of the process. The use of diagnostic models is augmented by more traditional expert system techniques to represent empirical or compiled process behavior. It is expected that this approach will provide an improvement in robustness over previous efforts that were based solely on rule-based expert systems.

Techniques for model based reasoning have also been researched by the German research organization Gesellschaft fur Reaktorsicherheit (GRS) resulting in diagnostic systems installed in the Biblis, Gundremmingen, and Phillipsburg

stations (Ref. 4.14). The main emphasis in this research work is the integration of symbolic and numerical reasoning through the development of appropriate dynamic knowledge structures.

FAULT EVALUATION AND FORMULATION OF MITIGATIVE STRATEGIES

The function of evaluation is to assess the nature and severity of the fault in order to formulate an appropriate corrective action. The trend worldwide in fault evaluation and the formulation of mitigative strategies has been largely to mechanize the operator response. An extensive amount of work has been done to develop a series of emergency response procedures that are explicit and complete enough to ensure proper operator response in all situations. In organizations that permit the operator to take an active role in the evaluation of faulted conditions, all the operator has to do is to get into the right procedure. In turn, it has become a goal of the computerized fault detection and diagnosis systems to assist specifically in this job of ensuring that the correct procedure is selected.

Reducing the role of the operator in fault evaluation to that of selecting the correct procedure to follow presents a number of developmental difficulties. The use of a preprogrammed set of emergency responses relies heavily on the ability of procedure designers to predict abnormal system behavior accurately and completely. The required knowledge of faulted process behavior must be developed by simulating system response to a large number of likely failures, then representing that abnormal behavior in an appropriate data structure against which a comparison may be made. This data structure, which is taught to the operator as a simple mapping exercise, relies on observation of a relatively small number of plant measurements. There are several difficulties inherent in this method that tend to lead some organizations to seek alternative approaches.

> There is no way to anticipate every failure that may occur in a process. Of necessity, therefore, the amount of knowledge that can be assembled concerning the external indication of system failure is limited. Each effort of this nature is station-specific and must be repeated in its entirety for a second station.
>
> It is difficult to predict accurately the course of system response in a quantitative manner because of the limitations of typical nuclear system models. It was found in the early work on nuclear station alarm trees that alarms are rarely received in a predictable and repeatable order for a given fault, and that small parametric changes in the initial conditions of a fault can produce large changes in the faulted system behavior.

A procedure-based strategy could be rendered ineffective if there were multiple faults, unless each possible combination of multiple faults was simulated and analyzed, or if there was unanticipated operator intervention with the operation of a process system assumed to be responding automatically.

Systems to Assist the Operator in Fault Assessment

In light of these difficulties with a preprogrammed fault response strategy, several European organizations have investigated the implications of providing the operator with additional information beyond predetermined emergency procedures to assist in fault assessment and mitigative strategy formulation.

EFD (Norway--OECD Halden Reactor Project). The first major aspect of fault evaluation is that of estimation of fault size or severity. The researchers at Halden have augmented the Early Fault Detection system described earlier to provide a predictive model capable of estimating the magnitude of a fault--for example, the size of a leak (Ref. 4.15). From this information, the operator is able to formulate an appropriate mitigative strategy that does not overreact to the fault. This feature does not add to the overhead of EFD, as the predictive model runs only after EFD has detected a fault.

The second major aspect of mitigation is the actual formulation of mitigative actions, a planning process. The panel found two examples of systems that are designed to assist the operator in this planning function.

ACACIA (France--Commissariat a l'Energie Atomique and Electricite de France). In France at CEA, Cadarache, and EdF, Lyon, a system called ACACIA has been developed to assist in formulating fault mitigative strategies (Ref. 5.16). The central part of this system is a knowledge base containing symptom based rules for fault mitigation. Implementation of this knowledge base makes use of distributed artificial intelligence techniques based on the blackboard architecture. Although such a system could be applied on-line for operator assistance, for which research continues, the application of ACACIA is currently for procedure design and verification.

ADVISE (Czechoslovakia--Nuclear Research Institute at Rez). At the Nuclear Research Institute, Rez, Czechoslovakia, a program called ADVISE is being developed to assist operators in much the same way as ACACIA. This system also provides an assessment of the severity of a fault. By monitoring the status of critical safety functions, ADVISE is able to present the operator with a range of options for mitigation.

FAULT MITIGATION SUPPORT SYSTEMS

The panel found in its review that two major approaches to the fault mitigation problem are being used in Europe. These include symptom-based response, as now commonly used in the United States, and event-based response, which requires some type of event recognition system in order to direct the automatic control system or the operators to the proper procedure.

Symptom-Based Fault Mitigative Systems

Symptom-based response has the advantage that the decision-making role of the operator consists mainly of rule-based reasoning thereby reducing the operator's cognitive load. The operator is required to follow a prescribed set of procedures when a certain pattern of faulted process behavior is observed. Symptom-based fault response is therefore effective only when the complete range of possible faulted behaviors has been discerned explicitly, a costly and difficult to verify task. The nuclear industry worldwide has invested great effort in providing for the quality of symptom-based procedures when it is decided that they will be used. Once an organization has adopted symptom-based procedures, it is possible to augment the traditional paper procedures involved in the task of fault mitigation by the use of computerized aids to operators performing these procedures. The panel observed several of these systems.

Computerized Emergency Procedures (France--Electricite de France). The approach to mitigation at EdF is that it is the responsibility of the operator to perform a specific set of actions in response to a fault. In order to support the operator in the performance of these mitigative actions, the new control room proposed for the next generation of French nuclear stations contains a computerized operating procedure manager. The purpose of this system is to guide the operator through a set of emergency procedures whose steps have been predetermined and validated.

At the Bugey training simulator where the prototype for this new control room is located, the panel saw a demonstration of this system. The operating procedure is presented to the operator as a sequence of logical boxes representing decision points and pathways, which reflect the progression through the logic of the procedure. Within each decision block, the operator is provided with information concerning the nature of the decision required and the source of the measurement information needed in order to make that decision. The operator's decisions are verified by the process computer, where possible, and if an incorrect path is chosen, it is so indicated by a contrasting pathway color.

COPMA (Norway--OECD Halden Research Project). A computerized operating procedure support system has also been developed at Halden (Ref. 4.17). This system, called COPMA, contains software development tools that simplify the conversion of procedures into structured software programs, and a logical reasoning system that supports the operator in performing procedural steps. A very effective graphical user interface supplements the procedural knowledge in the system.

Event-Based Fault Mitigative Support Systems

The second widespread methodology for fault mitigation is an event-based strategy. The operator or the computer chooses a specific event based on the observed process response, then proceeds to take mitigative action on the basis of that selected event. Typical events include specific equipment casualties (e.g., loss of a reactor coolant pump); traditional nuclear station emergency conditions (e.g., a loss of coolant accident); or external events originating at the plant process boundaries (e.g., disconnection from the electrical grid). These events must be recognized by diverse means in order to provide robustness in their recognition.

Limitations System (Germany--Siemens). Typical of an event-based system for response to process faults is the Limitations System used in German nuclear stations designed by Siemens. The Limitations Systems as a portion of the plant control strategy is discussed more fully in Chapter 5; however, from the standpoint of being an automatic fault mitigation system, it is worth mentioning as being typical of the approach that concludes that fault mitigation is too critical to be left mainly to actions of human operators. When a fault occurs in a plant with the Limitations System, the analog electronics are designed to map the occurrence of certain symptoms of faulted behavior to a specific fault event and then to initiate a set of automatic control actions that are taken in order to minimize the effect of the fault on the plant and to avoid a reactor trip. The principles upon which this system operates would most likely be realized in digital hardware and an algorithmic programming language should it be implemented in the United States.

Evidence shows that this approach is remarkably successful, not only in trip avoidance, but also in reducing the cognitive load on operators during faulted conditions. The Limitations System acts in concert with PRISCA, the knowledge based display system present in the control room, to provide the operator with the ability to track performance of the automatic controls as the fault is mitigated, by noting the status of critical parameters. PRISCA thus performs the functions of a Safety Parameter Display system as currently mandated for U. S. plants, but is more completely integrated with the plant control systems.

FAULT MITIGATION SUCCESS ASSURANCE SUPPORT SYSTEMS

Once the mitigative strategy has been formulated and execution has begun, it is necessary to track the performance of the process to ensure that mitigation is effective. This may be done by well designed graphical presentation systems, such as PRISCA mentioned above, or by knowledge based systems that provide additional cognitive support for the operator in ensuring that the recovery is proceeding in the expected manner. The panel observed several examples of such systems.

ACACIA (France--CEA) and ADVISE (Czechoslovakia--Nuclear Research Institute at Rez). The systems mentioned previously under fault evaluation, ACACIA and ADVISE, provide a framework for success assurance by providing an effective interface to the operator of the critical parameters that are indicative of the process returning to a safe condition. In this sense, these systems function like an augmented Safety Parameter Display System; that is, the display functions are combined with intelligence, so that the displayed information is prioritized

SAS II (Norway--OECD Halden Reactor Project). Another system that should be mentioned in the area of mitigation assurance is a system for post trip plant analysis developed at Halden, called SAS II. In the time immediately after a reactor trip, the operator is faced with ensuring that the plant is rendered into a safe state and that the trip itself was sufficient to mitigate the fault that caused it. SAS II is based on the use of critical safety functions and success paths, both of which are post trip analysis techniques developed in the United States. The researchers at Halden have placed within a very attractive graphical user interface, using analysis tools based on expert systems for assessing whether the plant critical safety function objectives are being met in the post trip period, and whether safety systems are functioning in accordance with their specifications. The system also embodies knowledge contained in emergency operating procedures that the operator is directed to follow in the post trip period.

INTEGRATION OF FAULT MANAGEMENT SUPPORT SYSTEMS

The panel saw in Europe two instances of research systems attempting to provide an integrated framework for a series of fault management support systems. An integrated framework is an important advance because work on computerized operator support systems for the various tasks of fault management has not generally been closely coordinated. This has led to the development of a series of unintegrated fault management tools that need to be put into a cooperative framework in order to interact most effectively with the operator.

ISACS (Norway--OECD Halden Reactor Project). The ISACS system (Ref. 4.18) being developed at Halden provides a graphical user interface and high level manager for the Halden-developed suite of computerized operator support systems previously discussed. The purposes of this integration are to provide a single access point for plant information to enter the fault management system and to provide for the cooperation of the various tools in assisting the operator. For example, when the alarm system HALO detects a fault, control is handed to the diagnostic system DISKET. If it is necessary that the operator then follow a procedure, that procedure is loaded into COPMA and presented to the operator for execution. This integrated framework is implemented within an expert system shell called G2, a powerful environment for the development of tools to monitor and manage process operation.

GRADIENT (Germany--ABB and ESPRIT). The GRADIENT project that is being sponsored by ESPRIT consists of an integrated framework for a set of expert systems under development at the ABB Heidelberg Research Center. Using Jens Rasmussen's model of human interaction (Ref. 4.16), GRADIENT establishes a communications framework for a set of expert system "specialists" that have various responsibilities in reasoning about the condition of the plant processes and directing the operator's attention to relevant information. This system has been applied mainly to fossil station applications, but the technology is relevant to nuclear power, particularly the methodology for establishing effective communication among a set of cooperating expert systems.

There is a trend for more widespread research into the integration of fault management tools to create a comprehensive framework for operator support. For example, a description of an integrated framework for fault management has been described recently by researchers at GRS (Ref. 4.19).

OTHER DIAGNOSTIC SYSTEMS

This chapter has been concerned with process fault management systems. The panel also observed many implementations of machinery condition monitoring and diagnostic systems in Europe. These systems monitor such parameters as rotating machinery vibration and temperature, noise signatures present on the signals from the ex-core neutron flux detectors, acoustic emissions from high pressure piping, loose part signatures within system pressure boundaries, and various electrical parameters. Most of the systems that the panel saw are commercially available products in Europe, and are similar to systems available in the United States. The conclusion of the panel with respect to such systems is that advanced condition monitoring equipment is integrated with plant operation better in Europe than in the United States, and the Europeans appear to have had more success in

identifying and avoiding significant mechanical and electrical failures through the use of condition monitoring.

SUMMARY

The panel's major conclusions concerning computerized operator support systems in European nuclear stations may be summarized as follows:

1. Operator confidence is increased when the computer acts as a partner in ensuring the safe operation of the plant. Even in cases where a substantial amount of the actual mitigative actions have been given over to the actions of automatic controls, operators can use knowledge based cognitive aids effectively to track the actions of the system in protecting itself. Knowledge of the progress of fault mitigation actions either gives the operator assurance that previous actions are adequate or points up the need for additional intervention.

2. Knowledge based systems are finding wide application in the area of process fault management. The robustness that knowledge based systems bring guarantees a higher level of success for a given investment in fault management system development.

3. A significantly greater effort is being expended in Europe than in the United States to develop and deploy advanced fault management systems. This is due in part to the more rapid computerization of European nuclear plants. It is also due to the much closer relationship between the European nuclear operating organizations and the organizations that are developing fault management support systems.

4. Much of the technology that the United States needs to support the actions of operators in faulted situations is available to us in the form of software systems already in advanced stages of development in Europe. Through cooperative agreements already in place, U. S. systems engineers can get access to most of the technology needed to implement these systems in U.S. nuclear stations. By making effective use of this existing technology, organizations such as the Electric Power Research Institute and the Institute for Nuclear Power Operation may encourage the adoption of innovative fault management techniques by U. S. utilities without large investments in time or R&D resources.

REFERENCES

1. Gallagher, J. M., *Disturbance Analysis and Surveillance System Scoping and Feasibility Study*, EPRI NP-2240, July, 1982.

2. Johnson, S. E., *DASS: A Decision Aid Integrating the Safety Parameter Display System and Emergency Functional Recovery Procedures*, EPRI NP-3595, August, 1984.

3. Pew, R. W., D. C. Miller, and C. E. Feeher, *Evaluation of Proposed Control Room Improvements Through Analysis of Critical Operator Decisions*, EPRI NP-1982, 1981.

4. Marshall, E., C. Reiersen, and F. Owre, "Operator Performance with the HALO II Advanced Alarm System for Nuclear Plants - A Comparative Study," in C. Majumdar, D. Majumdar, and J. Sackett (eds.), *Artificial Intelligence and Other Innovative Computer Applications in the Nuclear Industry*, Plenum Press, New York, 1988.

5. Kraft, M., G. Wohrle, and F. Pigler, "An Advanced Alarm and Data Management System for the 1300 MW Phillipsburg Nuclear Power Plant, Unit 2," presented at the ANS Conference on Applications of Computers in Nuclear Power, Pasco, 1985.

6. Prock, J., "Three Level Conception for Signal Validation and Early Fault Detection in Closed Systems," presented at the Enlarged Halden Group Meeting, Bolkesjo, Norway, 1990.

7. Jokineva, H., M. Lilja, and A. Sorenssen, "Early Fault Detection in a Real Nuclear Power Plant by Simulation Methods," ENC-90 paper no. 26/42.09, published in the Transactions of the ENS-90 Conference, pp. 1777-1781.

8. Bastl, W., "Integrated Disturbance Analysis, A Basis for Expert Systems in Nuclear Power Plants," in C. Majumdar, D. Majumdar, and J. Sackett, (eds.) *Artificial Intelligence and Other Innovative Computer Applications in the Nuclear Industry*, Plenum Press, New York, 1988.

9. Bastl, W., H. Schuller, and D. Wach, "High Performance and Safety of Nuclear Power Plants by Means of Early Fault Detection," IEAE-CN-49/4, presented at the Conference on Man Machine Interface in the Nuclear Industry, Vienna, 1988.

10. Ancelin, J., J. P. Gaussot, M. Gondran, and P. Legaud, "EXTRA: a Real Time Knowledge Based Monitoring System for a Nuclear Power Plant," IAEA-CN-49/66, Presented at the Conference on Man Machine Interface in the Nuclear Industry, Vienna, 1988.

11. Berg, O., and M. Yokobayashi, "Combination of Numeric and Symbolic Processing in Fault Detection and Diagnosis," Halden Report HWR-174, March, 1986.

12. Papin, B., P. Bernard, J. Tyran, G. Zwingelstein, and P. Bajard, "On Line Surveillance of Pressurized Water Reactors by Process Analysis," presented at the ANS Conference on Applications of Computers in Nuclear Power, Pasco, 1985.

13. Gorlin, A., A. Polyakov, and S. Semenov, "Some Applications of AI Technology in Nuclear Industry," IAEA Demonstration of Expert Systems Technology that took place in Moscow October 1-5, 1990.

14. Felkel, L., "Modeling Techniques for On-line Expert Systems in Nuclear Power Plants," presented at the ANS Topical Meeting on Advances in Human Factors Research and Man/Computer Interaction, Nashville, June, 1990.

15. Suzudo, T. and O. Berg, "On-Line Fault Size Estimation and Prognosis - An Operator Support System Demonstrated for the NORS Feedwater Preheaters," Halden Report HWR-236, April, 1989.

16. Rasmussen, J., "Outlines of a Hybrid Model of the Process Plant Operator," in T. Sheridan and G. Johannsen (eds.), *Monitoring Behavior and Supervisory Control*, Plenum Press, New York, 1976.

17. Krogsaeter, M., Larsen, J. S., Nilsen, S., W. R. Nelson, and F. Owre, "Computerized Procedures - the COPMA System - and Its Proposed Validation Program," Expert Systems Applications in the Electric Power Industry, Orlando EPRI Conference, 1989.

18. Haugset, K., O. Berg, N. T. Fordestrommen, J. Kvalem, and W. R. Nelson, "ISACS-1, The Prototype for an Advanced Control Room, " IAEA-SM-315/16, presented at the International Symposium on Balancing Automation and Human Action in Nuclear Power Plants, June, 1990.

19. Bastl, W. and H. Markl, "The Key Role of Advanced Man-Machine Systems for Future Nuclear Power Stations," IAEA-CN-49/56, presented at the conference on Man-Machine Interface in the Nuclear Industry, Vienna, 1988.

CHAPTER 5

CONTROL STRATEGIES AND TECHNIQUES

David D. Lanning

INTRODUCTION

This chapter focuses on the control strategies of pressurized water reactor (PWR) nuclear power plants. These strategies include methods for reactor control in the normal operating ranges and methods for reactor protection if the reactor or plant moves toward a limit of the operating range.

Review of Distributed Control of PWR Subsystems

As an introduction, it is useful to describe the PWR plant as a series of subsystems, each with some independent controllers, and all integrated within the total plant control. This distributed subsystem is depicted in Figure 5.1. It consists of the elements and controllers listed in Table 5.1.

The subsystem controllers of Figure 5.1 and Table 5.1 can be considered as a distributed control system, and all PWR plants have these same general features. There are, however, significant differences in the strategies for combining and operating these features and for imposing limitations on the plant operation if the system approaches the operating bounds. The PWR plant's system controllers in the past have been analog systems. Recently in some plants, digital microprocessors are being used to replace the analog systems.

This chapter describes first a typical control strategy, then a number of control strategies differences, and finally the progression toward advanced, digital, and more automated control features in France, Germany, the Soviet Union, and Czechoslovakia.

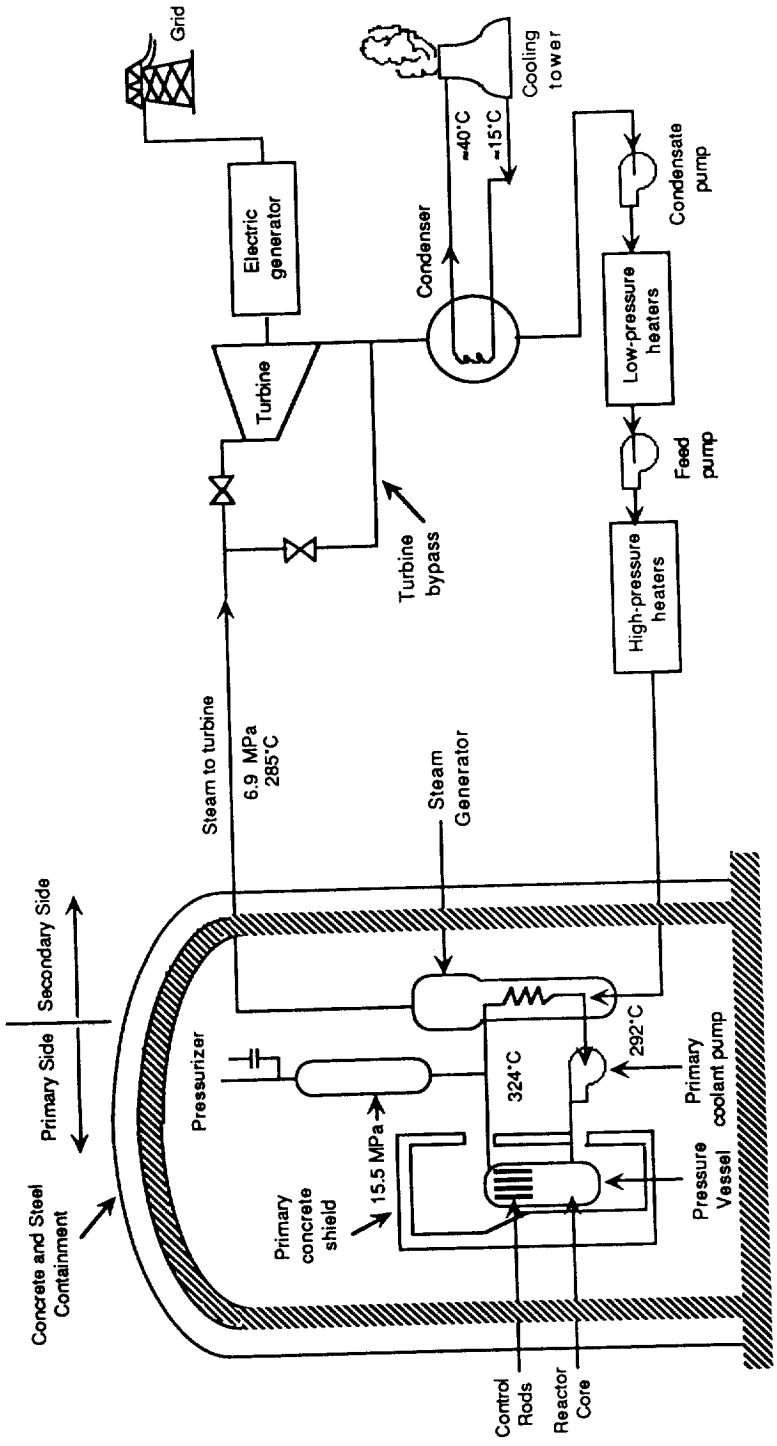


Fig. 5.1. Schematic of a PWR Power Plant

C-2

Table 5.1
Subsystems and Controllers of PWR Nuclear Power Plants

Subsystem	Controller
Reactor Core	Reactor power and thermal feedback reactivity effects are controlled by using neutron absorbing rods that can be moved into or out of the core. (Soluble boron, in the form of diluted boric acid, is also used for slower reactor control.)
Pressurizer	Pressure of the reactor coolant is controlled by adjustment in the pressurizer using spray or heater systems to lower or raise the pressure. Water level in the pressurizer is controlled by the letdown or makeup system changes to the primary system.
Steam Generator	Pressure on the secondary side of the steam generator is controlled by the turbine throttle and bypass valves, which regulate the steam from the steam generator. Water level on the secondary side is controlled by adjusting the feedwater flow rate to make up and match the steam removal rate. Feedwater comes from the condenser and passes through feedwater heaters, all of which have separate water level controllers.
Primary Pumps	Primary coolant flow is normally constant for PWR operation; pump operation is controlled at a steady state.
Turbine Generator	Electrical power output is a user-demand quantity. The turbine generator is operated at a constant shaft speed of rotation. A set of turbine and generator controllers adjust the electric output, cool the generator, protect against turbine overspeed, and adjust the turbine throttle valve to provide the first stage turbine pressure for a steady power operation at the desired electric load.

CONTROL STRATEGIES FOR PWR POWER PLANTS

A Typical Control Strategy

The distributed control subsystems presented in Figure 5.1 are typically connected as shown in Figure 5.2. The controllers shown on Figure 5.2 are described in the following paragraphs.

The pressurizer has two controllers, one for pressure and one for level. Inputs to these controllers are only from the pressurizer subsystem pressure and level readings; hence, the system integration is by the effects of the system response (no anticipatory control information). The output controls the appropriate system valves.

The steam generator level control has an input from the steam generator level and also from the steam generator steam flow rate and from the feedwater flow rate. If there is a mismatch in steam flow or feedwater flow, the controller can anticipate a level change and thus enhance the controller response. The output is a control of the feedwater flow control valve with a possible related effect on the pump speed control.

The reactor power level and power distribution controller have inputs from the neutron detectors around the core (ex-core), and in some designs, from detectors in the core. Also, there are input signals from the temperature of the primary coolant. Within the controller, part of the control integration includes a planned (i.e., demanded) temperature for the given power demand. In essence, there is some feedforward control calling for a reactor power increase when the working power level is increased. The output of the reactor power controller is the signal to the mechanisms that make the adjustments of control rod positions or the adjustments of the boron concentration (BRS on Fig. 5.2).

The steam flow to the turbine is controlled by adjusting the turbine inlet throttle valves and the turbine bypass valves. This controller receives input from the turbine first-stage pressure and the power demand. Again, the integrated control includes an established steam pressure and consequently a given steam flow and temperature for a given power demand. There are other controllers on the turbine generator system to provide a constant speed for the turbine shaft, the required cooling for the generator, and protection from overspeed and excessive vibration.

The user can demand a certain electric power production, and there are two additional control choices that a system designer considers for a given power demand: the primary coolant average temperature, and the secondary system steam generator pressure. These two choices are diagrammed in Figure 5.3.

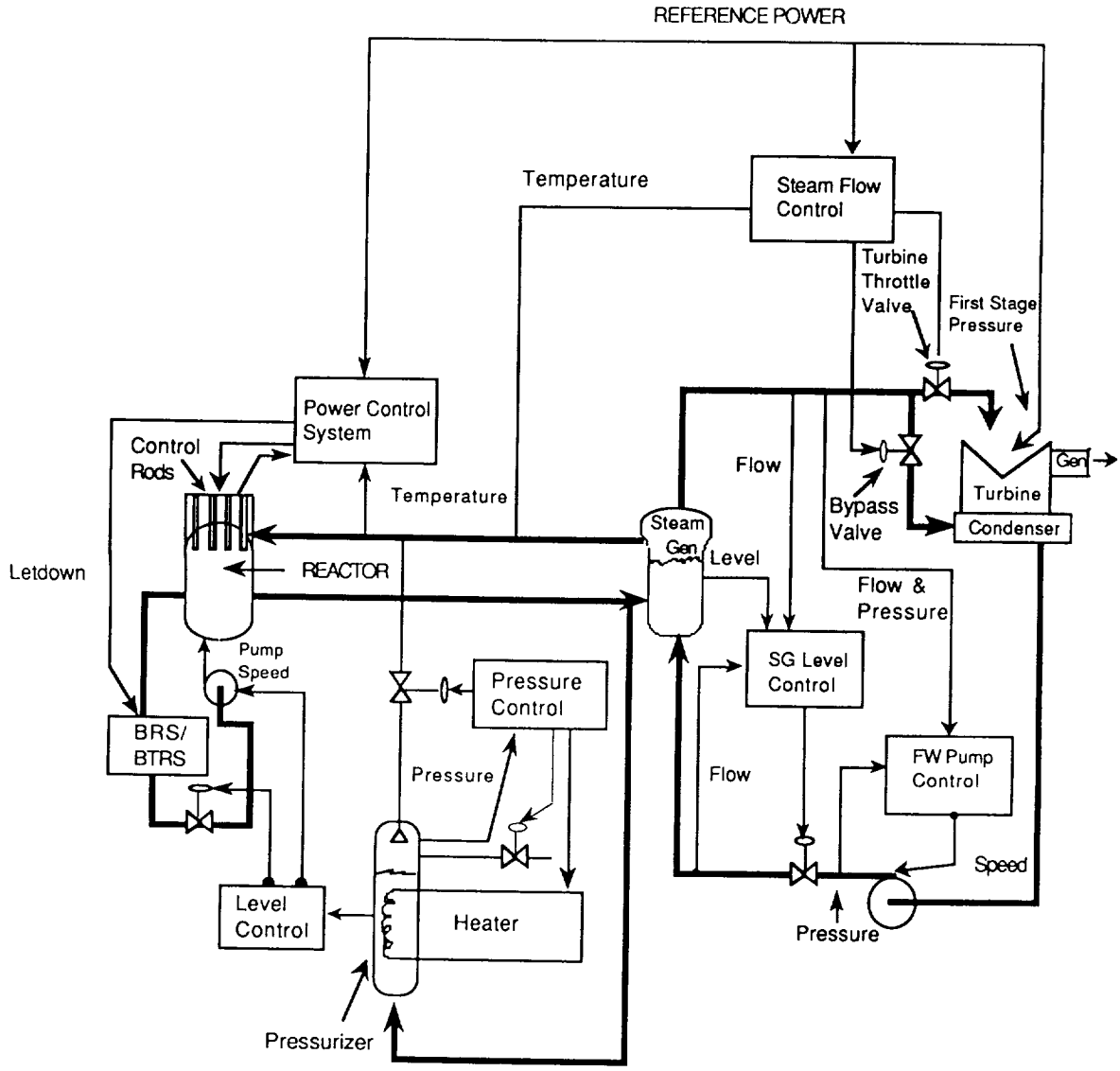
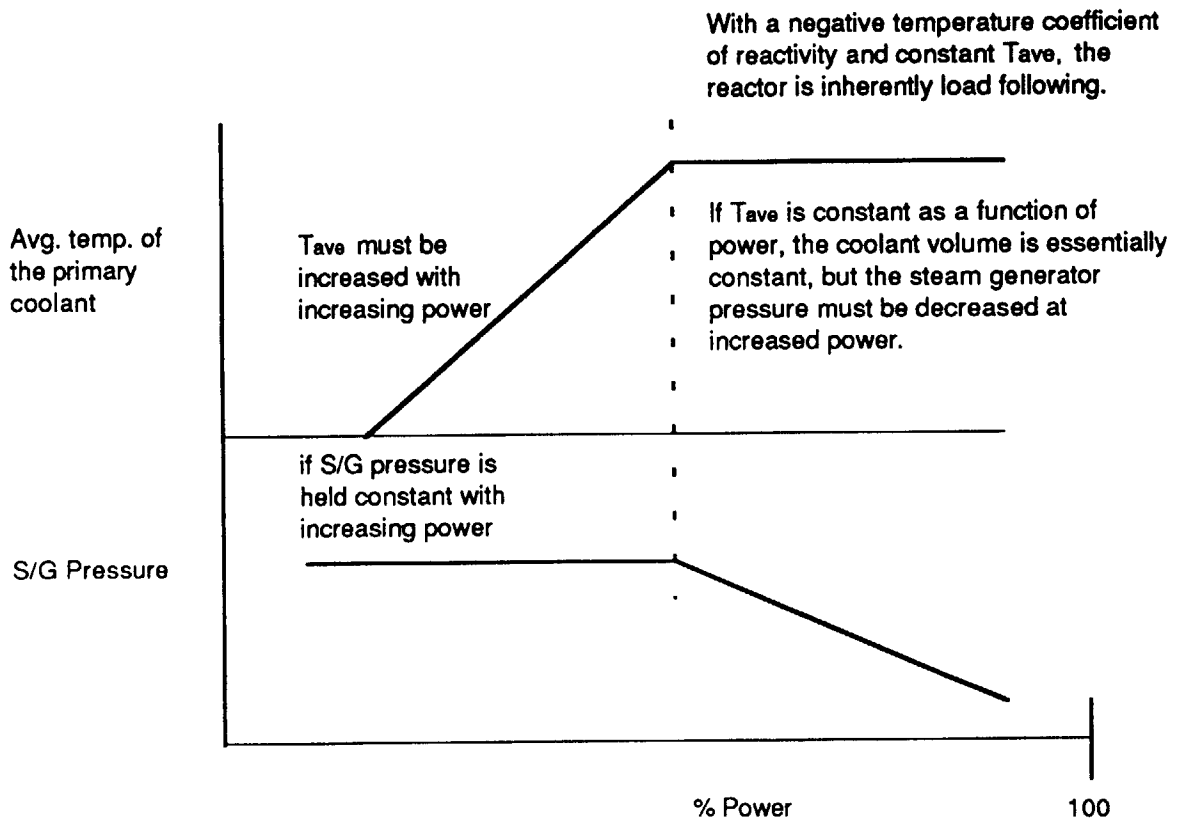


Figure 5.2. Typical Integration of Distributed Control Subsystems



Controllers are designed with various combinations of this regime.

Figure 5.3. A Possible Strategy for Programmed Control of Primary Coolant Temperature & Combined Steam Generator Pressure

Primary Coolant Average Temperature Considerations

Changing the temperature of the reactor core causes a change in the neutron chain reaction balance. This is called a reactivity effect, and normally the PWR systems operate in a boron concentration range such that the temperature feedback, i.e., temperature coefficient of reactivity, is negative. That is, decreasing the temperature increases the reactivity, and the power rises until the average core temperature is raised or the control mechanisms are adjusted. Since increasing the steam flow to increase the turbine power takes energy from the steam generator, the first system response is to decrease the primary temperature; this in turn increases the reactivity. Thus, there is an inherent tendency to cause the reactor to follow the turbine demand.

Other reactivity effects (e.g., Xenon absorption, Doppler feedback, and system response time) require adjustments in the control mechanisms to maintain the desired power. However, if the control strategy is to keep a constant average primary system temperature, the control of the reactor power is simplified and changes in the reactor coolant volume are minimized, thus reducing demands on other controllers such as the pressurizer and makeup system.

On the other hand, as shown in Figure 5.3, holding the reactor average temperature constant means that the pressure on the steam side of the steam generator (hence, secondary temperature, since the steam generator is at saturated conditions) must vary with power, being highest at lower power in order to attain the heat transfer from the primary system to the secondary system.

Secondary System Steam Generator Pressure Considerations

In general, the system designer does not want to design the secondary and balance-of-plant systems for the very high pressures that would be required at low power if the average primary temperature is held constant. This would mean that the system was overdesigned, since the system operates primarily in the higher power range. Hence, another control strategy is to keep the steam generator pressure constant at all power levels. This means the primary coolant average temperature must be increased whenever power is increased. As stated previously, this makes the reactor system control more complex and requires a larger range of preplanned control mechanism adjustments.

Comparison of Control Strategies

In the plants the panel reviewed, variations in the control strategies are largely tied to the degree of load following capability included in the plant operation. For plants with no or very slow load changing, the strategy is to hold the steam generator pressure nearly constant and program the primary system temperatures

nearly linearly, increasing the average temperature of the primary coolant with increased power demand. For plants designed to allow more load following, the strategy is to hold primary coolant temperatures nearly constant in the upper power range over which the load following will occur, and to hold the steam pressure constant if operation is taken to the lower power levels. This latter control strategy (depicted in Fig. 5.3) allows the plant to move through significant load changes in a rather short time without making large changes in the reactor control system. It therefore simplifies the assurance that power distributions within the core always stay within thermal limits.

Comparison of Operating Limitations and Safety Systems

It is important to protect the reactor in the event that system conditions approach the thermal limits (e.g., power too high, flow or pressure too low, or temperatures too high). The panel's review of control systems included discussion of the limitation and safety system strategies. Some interesting variations are briefly described below and summarized in Figure 5.4.

The French PWR safety systems are very similar to the U.S. systems. In these plants, the operating range is allowed to move closer to the trip condition. Alarms and information alert the operator if the trip limit is being approached; if a trip occurs, the control rods are inserted to shut the reactor down. A closer check on the approach to thermal limits can be made by using the digital system computing capability. Both the United States and France have developed such systems: in the United States, an example is Combustion Engineering's Core Protection Calculator (CPC) discussed further in Chapter 8; in France, the microprocessor safety system SPIN is used. The French experience base in the technology is much larger than that of the United States, as the SPIN system is being used in 23 plants.

In the German Konvoi PWR plants, the limitations system is a unique, automatic control arrangement. If the reactor state enters the limitation region, several types of control action may be initiated to move the reactor state back into the acceptable operating regime. (A further discussion of this limitation system is given in a later section of this chapter.) If the reactor state continues to move away from the operating regime, then a runback will be initiated, and if this is not sufficient, then a trip inserts all control rods to shut the reactor down. Almost always, the early action of the limitation system prevents the system from ever reaching the trip conditions.

The Soviet safety system for the VVER-type PWR plants is designed to give the largest existing margin between action limits and the true level of safety concern. As the system enters these action-limited regions (e.g., if the power rises too high),

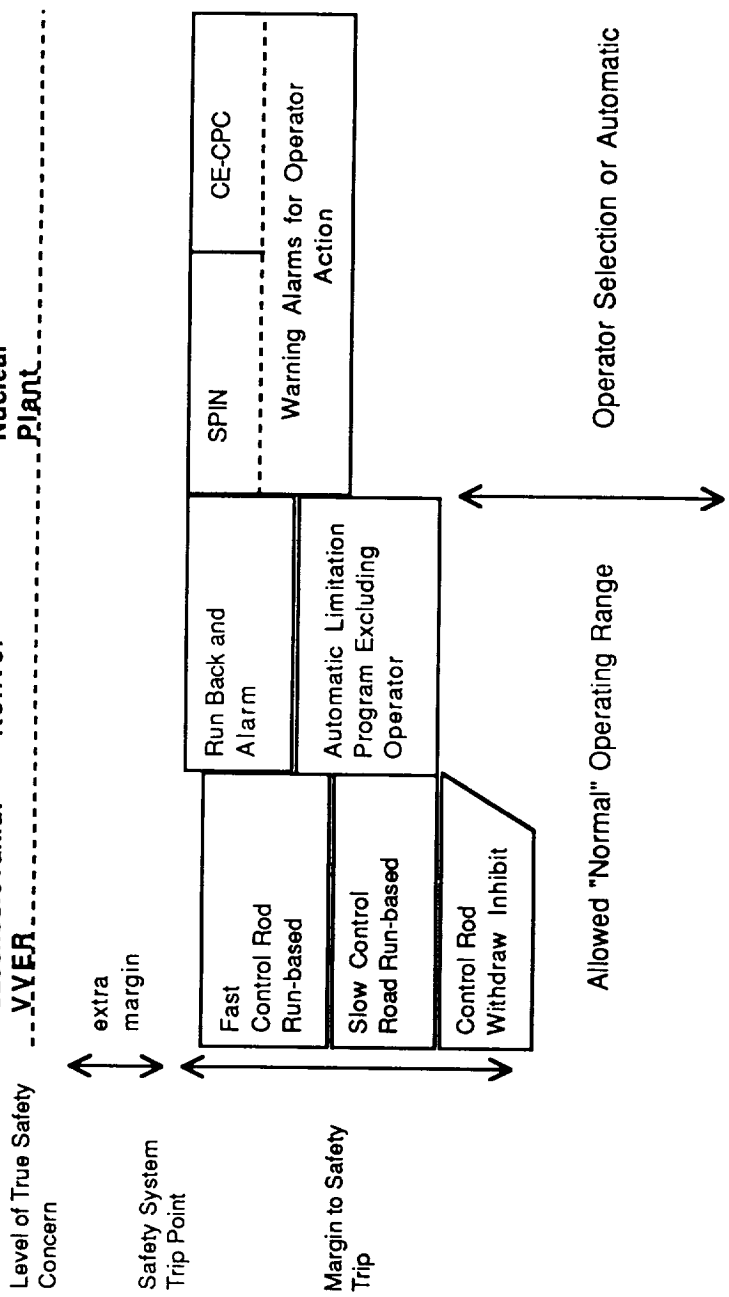


Figure 5.4. Comparison of Operating Limitations & Safety Systems

the system first starts a power runback by inserting control rods to reduce the power. If the power rises higher, rods are inserted at a greater rate. Finally, if the power continues to rise, the trip point is reached that drops all rods into the reactor to shut the reactor down. From the panel's discussions (Ref. 5.1), it appears that the trip point in Soviet plants is set at a more conservative thermal condition point than in other countries. Thus, although the technology of the control and safety system seems to be of the older analog type, the strategy for limitation and protection seems very robust and conservative.

COUNTRY-BY-COUNTRY ASSESSMENT OF CONTROL STRATEGIES

Control Strategies in French PWRs

Modes of control. Because the French generate 70 percent of their electricity in nuclear power plants, they need to be able to load follow with some nuclear plants (other countries normally base-load all of their nuclear plants). Originally the French nuclear plant control systems were based on the same designs as those used by Westinghouse in its PWR plants.

The Westinghouse control system the French call Control Mode A. By making certain evolutionary improvements, they have evolved a Control Mode G and recently a combined Control Mode X. These three control modes are listed in Table 5.2 (Refs. 5.2, 5.3). The Control Mode A involves use of standard full-length control rods with some boration concentration changes to avoid axial power peaking limits. The reactor temperature is programmed for a given power demand. This system is too slow for satisfactory load following.

For a safe, faster response, the French improved the axial ex-core monitoring system, going to six monitors. They improved control rod position indicators and developed special "gray" rods (reduced efficiency rods) that could be moved without causing large changes in power distribution. This control mode has been used successfully for load following more than 2500 times over the past few years (Ref. 5.4).

The new control mode, Mode X, was developed for use on N4 plants. It has been tested on present plants. This mode provides simultaneously closed loop control for both reactor coolant temperature (as in mode A) and axial offset by making use of "black" as well as "gray" rods. Temperature is controlled by moving rods which are inserted at a mid-core position and exhibit a high effect on the temperature and a low one on the axial offset. Axial offset is controlled by moving rods which are almost completely inserted or withdrawn, and therefore exhibit a low effect on the temperature and a high one on the axial offset. The Mode X Control has been developed for both load following and frequency control.

Experience with the frequency control has shown that PWR plants can hold to a 7 MWe band within the allowed 100 MWe control band (Ref. 5.4).

Table 5.2
France's Three Control Modes

Control strategies are based on the same principles used by Westinghouse in U.S. PWR systems.

Control modes have been extended to allow load following.

MODE A	The Westinghouse original mode is difficult to use for load following; rate of power change is too slow, involving changes in coolant boration.
MODE G	Control design includes "black" rods for closed loop temperature control as well as "gray" rods for open loop power control allowing load-follow and frequency control.
MODE X	Mode X can be used for load following and for frequency control (using mid-plane control for high reactivity effect with low axial effect). In this mode, both temperature and axial offset are closed loop with a combined use of "black" and "gray" rods.

Digital Microprocessor Reactor Protection Systems. French experience in the use of digital microprocessors for control and protection is the largest in the world. The heart of their digital protection system is called the SPIN system.

SPIN takes signals from process instrumentation (temperature and pressure), nuclear instrumentation, and the control rod positions; this information is analyzed by the digital microprocessors. Global conditions such as pressures, temperatures, and power level, plus local core conditions such as linear heat generation rate and approach to departure from nucleate boiling (DNBR), are checked against predetermined limits. If any limits are approached, the operators are alerted. If limits are exceeded, then the SPIN output signals are sent to the controller of the appropriate protection and safeguards function, such as reactor trip (e.g., control rod drop) systems, safety injection systems, and emergency feedwater system. This SPIN system has been operating successfully in 20 of the French PWR units, of the 1300 MWe type. The operating experience amounts to 60 reactor-years.

In addition to the digital protection system, the recent French integrated control system utilizes digital processing in its automatic control system (Refs. 5.5, 5.6).

N4 PWR Plant and Advanced Control. France's large experience base in the use of digital systems is now being used for the advanced system being developed for the next generation of French PWR plants, the N4 plants. (The first N4 plant, Chooz B1, is designed for 1,475 MWe.) Some of the panel members visited the S3C simulator for the N4 plant control room and control system. The simulator is located at the Training Center on the Bugey Nuclear Plant site, where panel members were also shown the simulation and actual control rooms of present operating plants.

The control system simulated by the S3C/N4 is a "Computerized Control Room" with three workstations, each consisting of three video (CRT) color graphic display units with three touch panels, a tracker ball, and a function keyboard. The operator can choose a new display from a menu (and touch panel), or from tracker ball designation, or from a screen being displayed. Panelists were told that there are available 17000 displays, roughly 10000 technical screens, 3300 alarm sheets, and 3000 procedure sheets with flow charts and 700 operation displays (circuits). The large selection of displays allows specific displays to support each individual operator task with this CRT-based control system. The plant control operation can be performed from this console by pointing to the object on the screen (using the tracker ball) or by entering the label on the keyboard and then selecting the control on a control menu. Finally, the action is initiated by validation with a function key. Computerized procedures guide the operator through the proper sequential steps of any control action, and the operation enables the procedural step through the touch screen. It takes 1.5 seconds to go from screen to screen; for screens with realtime data (temperature pressures and flow rates), the screen can be updated in 50 msec, and the data collection time may be about 300 msec. The level of automation for the N4 plants will be the same as in the preceding systems (Ref. 5.6).

The implementation of the advanced digital control system has proven to be more challenging than originally expected. Recent developments indicate that the "Controbloc P20" (Ref. 5.7) has not been approved for operation in Chooz B and may cause a delay in the program (Ref. 5.8). In part, this problem seems to be due to the added complexity that can easily crop up when designers try to take full advantage of programmable systems. These problems occur in standardization as well as verification and validation of the software in order to obtain approvals. However, our host from France (Ref. 5.4) did point out that the CO3 (core instrumentation and control) section of the system has been qualified. The CO3 section involves reactor protection, nuclear instrumentation and control, and incorporates the SPIN system. Work is in progress relative to the qualification or

design modification and qualification of the remaining P20 system. (More information on this subject is given in Chapter 6.)

Control Strategies in German PWRs

In the area of control strategies and techniques, the panel's visit to Germany was focused on the Konvoi-type PWR, a Siemens-KWU 1300 MWe nuclear power plant. This review also included a visit to the Isar-2 plant near Munich.

Global control. The control strategy in Germany incorporates a high level of automation (Refs. 5.9, 5.10)) for both the operating range and the marginal region called the limitation region. The strategy for global control over the power range from about 40% to 100% is to hold the average primary coolant temperature constant. That is, the reactor nearly inherently follows the turbine demand, and control is such that the average primary coolant temperature is constant, and the secondary system is designed to operate at higher pressures during part-load conditions (see section above on operating limitations). Below 40% power, the control strategy changes to a programmed primary coolant temperature such that the pressure from the steam generator is held constant. The global control includes ex-core neutron detectors for neutronic power information.

Local control. To assure that local conditions within the reactor core do not exceed thermal limits (i.e., linear heat rate), DNB, or PCI (pellet-clad interactions), there is also a local power control. Local power information is monitored by use of an in-core realtime monitoring system consisting of cobalt prompt-responding, self-powered detectors. Periodic calibration of the in-core detector system is provided by a sophisticated "aeroball" activation measuring system. The aeroball system pneumatically inserts vertical columns of small metal balls into tubes in the core. These balls are irradiated for three minutes and then pneumatically removed to an automatic counting array. A core power distribution map is generated in about ten minutes.

The combination of global and local core monitoring allows the control strategy to include "full load-follow" capability; that is, it allows for fully automated load changes and operation in the power range from 25% to 100% of full load (Refs. 5.9, 5.10). Information on this controller indicates that frequency control has also been demonstrated, that is, the plant was allowed to automatically respond to frequency changes by changing the generator output. Frequency control involves rapid power response with limited load changes (<100 MWe) over a time frame of minutes, whereas the load follow involves rates of change of load preset by the operator in the range of 2% per minute to 10% per minute and a new target power setting in the range of 25-100%, with a time frame of hours.

Limitations system. The Konvoi type control and protection systems are much more integrated than any other system in the United States or Europe that the panel reviewed. An important part of the automatic operation is incorporated with the "limitations system." This layered operation and protection strategy (shown in Fig. 5.4) is unique in that the limitation system takes control away from the operator or away from the normal automatic controller if any limit is being approached. The automatic action to move the plant condition back to the acceptable operating range is less stressful than a complete reactor trip. The closer the plant approaches limits, the more rigorous the limitation control takes automatic action until at the limit a reactor trip is taken. The limitation systems are fault tolerant through multiple redundancy (four power trains). The general strategy of this integrated control has been in operation for more than 15 years, and successful experience has developed to the extent that load change operation by remote control from load dispatching center (secondary control) can be allowed for load following.

The panel was able to observe the capability of this system in a simulator demonstration in the Siemens office at Karlstein. A series of transients were successfully handled, including dropping full off-site load and lowering power to house load without a plant trip.

Information displays. The operator's role in the German strategy becomes more that of a plant manager and accident manager. The operator needs in-depth knowledge of the plant operation and control status; therefore, information displays are an important part of the system. Special graphics are displayed on an array of color monitor video screens that present the status of the plant in terms of the normal operating range and the limitation region.

An example of one of these screens is shown in Figure 5.5. This figure shows the primary coolant pressure and temperature condition. At startup, the pressure must be kept low when the temperature is low to avoid the brittle fracture condition (NDT limit), but also the temperature cannot be too high at a given pressure to avoid boiling condition or pump suction head limitations (NPSH limit). Thus, a given normal operating band is plotted, surrounded on either side by the limitation band. The operating status is shown with a white dot, and a historical trend is plotted. Other pertinent information and prompts are indicated beside the main plot.

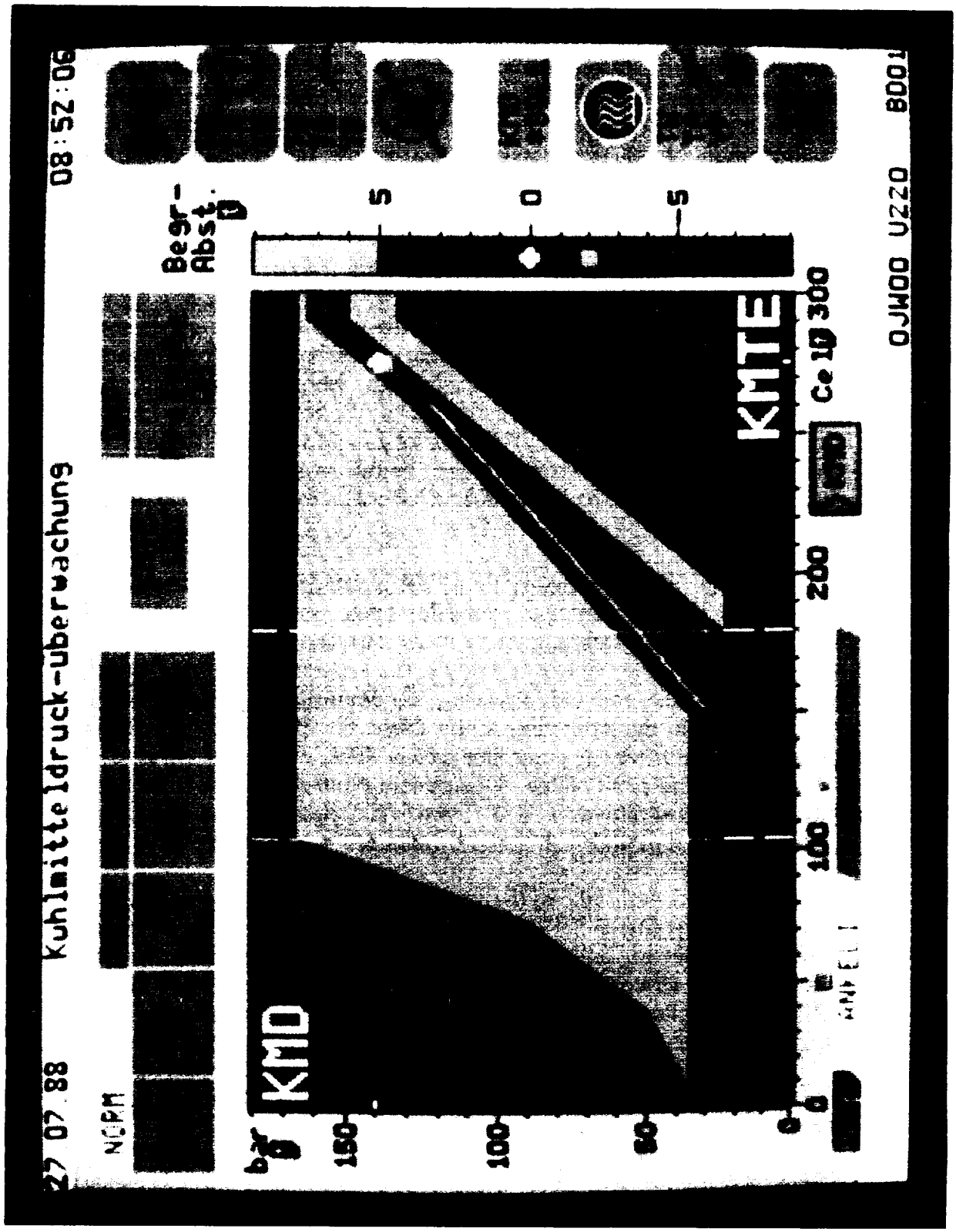


Figure 5.8. German Control Room Monitor, Showing Status of Primary Coolant Pressure and Temperature

The present operating systems with this integrated control strategy are primarily based on semiconductor equipment for analog (relays) and binary (on/off switch) functions. Although the operating experience has been very successful, the four-train design involves a very large array of racks (hundreds), each containing multiple replaceable cards, so considerable maintenance is required. Work is now in progress to implement these systems by using a new generation of digital instrumentation and control systems (Ref. 5.11). The same functionality and philosophy of fault tolerance with layered control strategies will be utilized.

Control Strategies in Soviet and Czechoslovak VVER-type PWRs

The panel divided into two groups after visiting Germany. One group went to Moscow and talked to the Soviet experts in nuclear power plant instrumentation and control. The other group visited Czechoslovakia, where it met with I&C experts in Prague and visited several sites, including the Dukovany nuclear power plant (four Soviet-designed 440 MWe VVER units of the 213 series) (Ref. 5.12). The Czechoslovak control strategies described below are essentially Soviet strategies, based on Soviet VVER-type PWRs and Czechoslovak for the balance of the plant.

VVER-440 strategies. The control strategy for VVER plants in Czechoslovakia is primarily based on use of these nuclear plants for base load and not for load following. This is in part due to rate-of-change limits imposed by the fuel design. In the VVER-440 (213 Series), the control strategy is the turbine follow type, where the reactor follows the turbine demand; however, the control is established for a constant throttle pressure in the operating range (Refs. 5.1, 5.13). These plants use a Soviet-designed reactor power controller called ARM, which has a variable structure that depends on the plant status. Component control systems are of the standard proportional-integral-derivative (PID) type. The present control system is not a complete closed loop, and well-trained operators are required.

VVER-1000 strategies. For the 1000 MWe type VVER, the Czechoslovaks are working on a control strategy that includes a constant average coolant temperature from 70% to 100% of full power; below 70%, they use constant throttle pressure. Thus, theirs is a combined strategy as described earlier. In the 1000 MWe plant, the advanced ARM-5 controller includes local control based on distributed in-core detectors, and automatic load following is possible.

As described previously and shown in Figure 5.4, the Soviet VVER systems are operated with a large margin to nucleate boiling. Also, the cores operate with a large negative temperature coefficient of reactivity, even with the maximum boric acid control. Thus, the control and safety systems are robust with large margins to safety limits.

The VVER-440 safety system is a type of limitation system: Level 1 is a reactor scram (rod drop times of 7 to 10 seconds plus I&C delay; for the 1,000 MWe the rod drop time is 4 seconds); Level 2 is a rapid rod insertion; Level 3 is rod insertion at normal rate (2 cm/s); Level 4 is a rod inhibit preventing withdrawal. For the VVER-1000 MWe, the system is similar but consists of three levels, omitting Level 2, the fast rod insertion. Safety and control rod systems are completely separate and have no need for signal isolation. The present technology for control implementation on VVER plants is primarily analog and binary, with very little use of digital systems.

Czechoslovak upgrade plans. As noted above, the Czechoslovak VVER plants use Soviet technology for the reactor control and safety systems and Czechoslovak technology for the control in the balance of the plant. Panel members were given an excellent tour of the control room and auxiliary control areas at the Dukovany Plant. The unit visited was in full operation. The control technology looked older than the plant (started 1986), and the panel was told that the I&C is the weakest (as well as the oldest) part of the system. There are high-priority plans to upgrade the equipment. Our hosts indicated an interest in Western equipment, but there would be difficulties with compatibility, new wiring requirements, and differing philosophies.

Czechoslovakia recently made an agreement with Siemens-KWU for some instrumentation on the Mochovice Plant (Ref. 5.14). The panel was informed that this will be control and instrumentation of the Konvoi type, except for the safety system. In order to retain fuel warranties, the plant will continue to use the Soviet safety system and will use essentially the Type 213 hybrid logic rather than digital. The turbine control system will be from Skoda in Czechoslovakia. Digital systems are being planned for the future (Ref. 5.1).

GENERAL ASSESSMENT AND CONCLUSIONS

Degree of Automation

The degree of automation is higher in European PWR plants than in present U.S. plants. This is true for both control and safety. In control, the capability to load follow has evolved most in France and Germany. In the safety area, Europe has added more margin; for example, there is a design rule that requires automatic action to take care of the reactor safety for 30 minutes after a reactor trip without operator assistance. This rule applies over the spectrum of accidents including loss of coolant. The panel was told that this rule applies also to VVER designs. In the United States, the time before requiring operator action is shorter, on the order of 15 minutes.

The panel was informed during the discussions in the European countries visited that, in general, the trend is expected to be toward even greater automation of the control systems. The role of the operator will become more that of a plant manager, requiring a higher level of education and deep knowledge of the systems through both education and simulator training.

The Arguments for More Automation

The panel heard the following arguments in Europe in favor of greater automation in the control and safety systems of nuclear plants:

> Automatic systems remember routine, detailed procedures and sequences better and faster than human operators.
>
> In periods of stress, operators do not have to make decisions but can check to see if the automatic system decisions are correct.
>
> Maintenance of the fault-tolerant automatic system can be made during periods of less stress.

Together with these arguments for more automation, the panel also heard concern expressed that with greater automation the operators will be less in touch with the real condition of the plant and may not be properly prepared or attentive if an emergency beyond the capability of the automatic system should arise. Further study on this aspect of the man-machine interface is in progress (see Chapter 2).

Outstanding European Control Strategy and Implementation Features

France has the most advanced use of programmable digital microprocessors in nuclear plant control and safety systems. Its digital systems include the implementation of step-wise operating procedures completely controlled through the digital systems but only enabled by operator demand, with information available through menu selection from 17000 video displays. The displays give realtime system status information and procedures with operator prompts.

Germany's PWR control and safety system for the Siemens-KWU Konvoi series is the most automated system of integrated control and protection function for nuclear power plants. The combined automatic controller, limitations control, and safety control move the operators the most toward being managers, observers, and maintenance coordinators. This system requires deep knowledge; such information is provided to the operators in terms of video displays of system function for integrated realtime functional analysis.

Soviet VVER-440 MWe (213 Series) and VVER-1000 MWe plants operate within robust control and safety regimes with large margins to limits. Soviet research into control theory is analytically advanced as compared to control theory studies in other countries (e.g., Ref. 5.15).

Future Control Strategies

In all of the European countries that the panel visited, the control strategies for the PWR plants are very similar to each other and also similar to the normal operating control strategy that is used in the United States. The move to the use of digital, programmable microprocessors has opened the possibility for future changes in control strategy (Ref. 5.16). Studies and research projects related to the development and use of accurate "realtime" simulation models are in progress in all countries. Simulation modeling has been used for several years in the production of full-scope training simulators. The possibility is now recognized that use of such realtime or faster-than-realtime models can be made to give improved control strategies that can cope with the nonlinear nature of nuclear power plant control.

In discussions with members of the European nuclear community, panelists heard about several research projects and plans to incorporate the results from calculations with realtime models of components and of the power plant for the following purposes:

Analytic redundancy. This method provides a comparable estimate of a sensor signal for sensor fault detection and estimation through consistency checks.

Fault diagnosis. The deviation from expected behavior might be quickly identified and diagnosed by comparison of the plant response with the accurate analytical model response.

Model-based controllers. The use of fast, accurate analytic models to guide the control action can overcome nonlinear control problems and can be developed in a hierarchical system to be self-protecting, hence never approach the trip points.

Logic-based information to provide operators with suggested best procedures for a given plant status. The computer model can be used to generate graphic displays for deep information, and systems might also be developed with logic to interpret the information, thus further assisting the operators or providing very advanced control.

Some interesting specific examples of these developments were observed in France at the CEA-Cadarache Research Center and in Norway at the Halden Research Center. At Cadarache, successful tests of a model-based controller have recently been demonstrated on a simulator (Refs. 5.17, 5.18), and advanced research is in progress on the possibility of developing emergency procedures in realtime by using the combined computer-gathered plant status and the symptom-based emergency operating rules (Refs. 5.19, 5.20). At Halden, the use of model-based information is being studied with emphasis on the man-machine interface (Ref. 5.21). In Russia and in Czechoslovakia, work is in progress on a wide scope of realtime models with emphasis at this time on development of accurate training simulators (Refs. 5.22 - 5.24).

In the United States, there is research in progress at national laboratories (Ref. 5.25) and at universities (Ref. 5.26) in this area of realtime models for advanced control. However, there is very little interest on the part of utilities in changing the present system of control or control strategies, even though some changes to digital systems have been made when commercial analog systems were no longer available. If new nuclear plants are purchased in the future, more consideration for commercial implementation of the advanced control strategies and automation is expected to occur. Thus, at present, the U.S. utilities operate their nuclear power plants primarily as base load plants. The United States depends heavily on highly trained operators. France and Germany are more advanced in the use of automation and in the development of future digital microprocessor systems for both control and protection.

REFERENCES

1. Information given to the panel in a meeting in Prague, 12/31/90.

2. Information presented to panel by A. Parry of Framatome La Defense, Paris, 11/26/90.

3. Framatome Group. "Experience Feedback after Six Years of Load Following Operations" (brochure) 1990.

4. Comments from French Host at the NSF workshop, 1/31/91.

5. Information presented to the panel by Mr. E. Pilaud at Merlin Gerin, Grenoble, France, 12/5/90.

6. Électricité de France. "Evolution of Operating System for Electronuclear Power Plants at EDF." Handout presented to panel by M. Combe and M. Montmayeul, 11/27/90.

7. Cegelec. "CEGELEC in the Nuclear Field." Informational handout.

8. *Nucleonics Week* 32 (No. 1, 3 January 1991).

9. Aleite, W. "Full Load-Follow Capability of KWU PWR NPP by Full Automatic Power Control." IFAC Symposium 12/15, Power System and Control. Beijing, August 1986,

10. Aleite, W. "Remarks about 'Why' and 'How' of KWU Konvoi PRINS." IAEA Specialists Meeting on Operational Experience with Control and Instrumentation Systems in Nuclear Power Plants, Brussels, Belgium, November 1987.

11. Hofman, H., H. D. Fischer, K. Lochner, and U. Mertens. "Microprocessor-based Information and Control System for Safety and Non-safety Applications in Nuclear Plants of the Nineties." ENC 90. Lyon, France, 23-28 September 1990.

12. See *Nuclear Eng. Int.*, Oct. 1990, p. 76 for a good description of major differences between the older VVER 230 Series and the enhanced safety of the 213 Series plus differences and improvements for the VVER 1000 MWe plant.

13. Stirsky, P. "National Report on Nuclear Power Plant Control and Instrumentation in Czechoslovakia." International Working Group on Nuclear Power Plant Control and Instrumentation/ING-NPPCI-IAEA. Munich, Oct. 1982.

14. "Mochovice I&C Contract Goes to KWU." *Nuclear Eng. Int.* p.3 (Nov. 1990).

15. Buner, D., F. F. Pashchenko, N. P. Kolev, and R. Tsvetanov. "Adaptive Algorithms for VVER Reactor Core Surveillance." *Modelling Simulation and Control, B.* Vol. 18, No. 1. pp. 19-30. AMSE Press.

16. Remarks on future plans were given to the panel members during meetings.

17. Information presented to panel by B. Papin of CEA-Cadarache, 11/28/90.

18. Papin, B., A. Poujol, M. Beolet, M., Beltranda. "An Advanced Concept for Nuclear Plant Hierarchical Control: SYCOMORE." Paper given to panel 11/28/90.

19. Poujol, A., B. Papin (CEA), and R. Soldermann (EDF). "Dynamic Synthesis of Emergency Operating Procedures Based on Generalized State Approach." IWRG on MMI, IAEA, Schliersee, RFA, 18-20 October 1988.

20. Papin, B., and R. Soldermann. "Display of Accident Operating Conditions Procedures Based on Generalized State Approach for Computerized Control Rooms." Paper received by the panel on 11/28/90.

21. OECD Halden Reactor Project (Ness, Eyvind, Berg, Oivind, Sorenson, Aimar.) "Early Detection and Diagnosis of Plant Anomalies Using Parallel Simulation and Knowledge Engineering Techniques." Paper given to panel 12/5/90.

22. Tsventanov, R., F. F. Pashchenko, and N. P. Kolev. "Algorithms for Estimation of Assembly-wide Power Distribution in VVER Type Reactors." Paper given to the panel on 12/4/90.

23. Gorlin, A. and S. Semenov. "Range of Expert Systems for Control, Modeling, and Safety Operation in Nuclear Energy." Paper given to the panel during the visit to Moscow, 12/4/90.

24. Krcek, V. and J. Leicman. "Developing and Upgrading Full-Scope Systems in Czechoslovakia." *Nuclear Eng. Int.* p. 48 (July 1990).

25. Rovene, L. A. (U. of Tenn.), P. J. Otoday, and C. R. Brittain (ORNL). "Development of a Robust Model-Based Reactivity Control System." Canadian Nuclear Society Third International Conference on Simulation Methods in Nuclear Engineering, Montreal, Canada, 18-20 April 1990.

26. Aviles, B. N. "Digital Control Strategies for Spatially-Dependent Reactor Cores with Thermal-Hydraulic Feedback." Ph.D. thesis, Dept. of Nuclear Engineering, Mass. Inst. of Technology, Cambridge, MA, February 1990.

CHAPTER 6

AN INVESTIGATION OF NUCLEAR POWER PLANT I&C ARCHITECTURE

James D. White

INTRODUCTION

The architecture of a nuclear power plant's control and instrumentation (I&C) system is a vital contributor to the success of the plant's design. This is now a very important subject in the field of nuclear power because new developments are being incorporated in architecture designs in many countries, including the United States. In some cases, these developments are only minor advances technically, whereas in others, these new developments may represent significant changes. The development and testing of the I&C system's architecture may be much more expensive than the cost of the system hardware; therefore, the successes and difficulties experienced by colleagues in the use of new designs warrant a designer's careful attention.

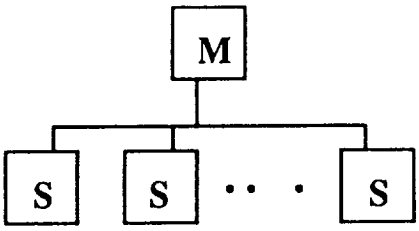
Definition of Architecture of I&C Systems for Nuclear Power Plants

In the case of control and information systems, the term architecture means the arrangement of control components, sensors, display devices, and communication devices. It also includes the arrangement of the information (or data) and the arrangement of the software in the case of digital systems.

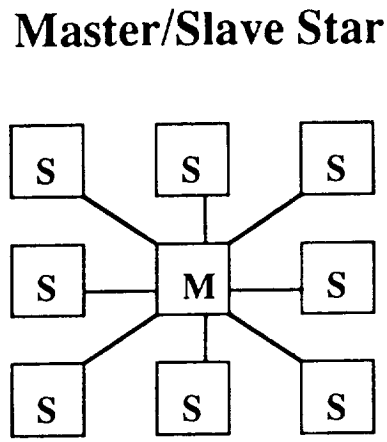
For those readers who may not be familiar with architectures, some simple, generic examples of hardware architecture are given here. Shown in Figure 6.1a is a diagram of a very simple control architecture in which there are one master controller and several slave controllers. The master is at the top level of the control hierarchy and the slaves are at the second (and last) layer of control. The master communicates with the slaves by sending commands onto a communication network shared by all of the slaves. Figure 6.1b shows another type of

architecture in which one master communicates directly with each slave controller on individual communication channels.

In Figure 6.2a, an architecture is shown that uses communication bus masters on several communication channels, or buses. For each communication bus, one master controller commands the slave units attached to that bus. A different type of architecture, shown in Figure 6.2b, uses a ring arrangement of components in which each component puts information onto the ring and takes information from the ring.

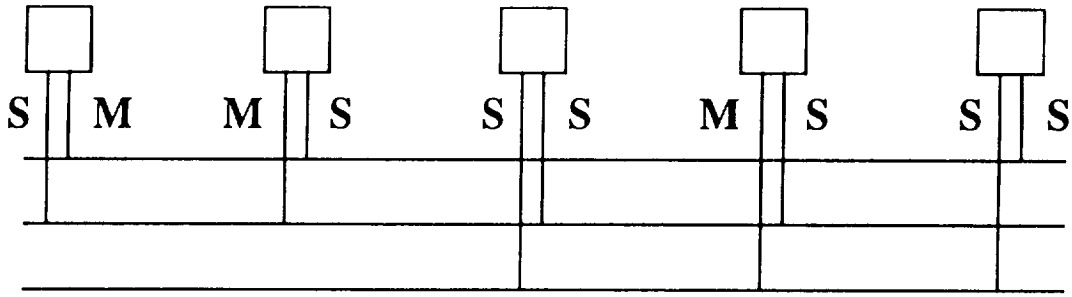


6.1a



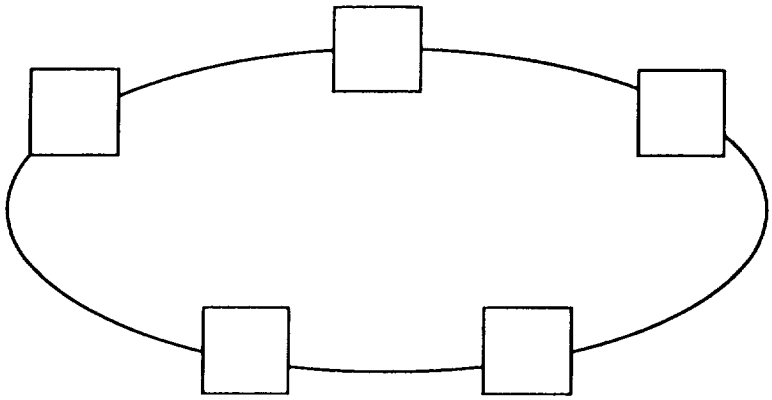
6.1b

Figure 6.1. Simple Examples of Hardware Architecture



Communication Bus Masters

6.2a



Ring

6.2b

Figure 6.2. Other Basic Types of Architecture

Architecture Design Issues

Each of the types of architecture shown in Figures 6.1 and 6.2 has advantages and disadvantages for particular applications. The designer chooses the architecture that best satisfies all of the requirements of the system. Architecture designs must address several types of issues; as a result, the architecture of a power plant control or information system generally is a combination of several types of simpler architectures into a larger, complex whole. For purposes of this discussion, the design issues are grouped into seven categories:

1. *User.* The first category includes questions about user interaction with the architecture, ease of understanding, ease of analysis of failure modes, and security.

2. *Allocation of requirements.* This category includes selection of networks, hardware, and software that will fulfill the overall requirements in an efficient manner. This involves choosing which requirements are allocated to which parts of the architecture and which parts are backups for other parts. A distinction is made here between "distributed computers" and "distributed computing." The term distributed computers means a hardware arrangement where only computational results or end points are shared. It does not consider distributing the computational functions.

3. *Database.* This category includes data management, sharing (or isolation), and storage of information. Reliable, high-capacity databases are required for good information engineering designs.

4. *Standards.* There is no one standard for a power plant architecture. The designer must choose which parts of which standards are applicable to each part of the architecture.

5. *Performance.* The requirements of the architecture must be met in a reliable, timely manner. The designer must decide how to get satisfactory throughput, response time, reliability, and fault isolation. Fast communication buses are necessary to handle the increased amounts of data and control signals. If the designer increases information density within single devices of the architecture, there may be greater consequences of device failure. An in-depth analysis has to be done to determine which tasks have to be implemented independently. If the designer includes a great deal of serial processing of programs, the reaction time of the system will be impacted.

6. *Adaptation.* As the plant ages, requirements for the control and information system will change. For good long-term economic performance, it is essential that the architecture remain open to evolution. Design lifetimes of

60 years and more are being proposed by reactor designers. The technology is moving fast. It is probable that some new technology will give added capability with significant improvements in safety margins and economics. The designer would like to choose an architecture which will allow future upgrading and modification.

This issue also involves the question of open architectures. Computer vendors are beginning to design systems that are easier to interface with systems of other vendors than in the past; this tendency is expected to continue. An architecture may be described as open if products from more than one supplier can easily be integrated. Although this does not seem to exist today in nuclear power plant architectures in the strict sense of the definition, it is a desirable feature that some U.S. utilities are beginning to request in meetings with the Electric Power Research Institute.

7. *Management.* Of course, one of the most important issues is cost. Trade-offs between layers of redundancy (for increased fault tolerance) and costs are difficult design decisions. How much the control is decentralized or centralized is another important design question. Centralized control may be simpler and cheaper, but decentralized control may be more fault tolerant and more amenable to modification. Maintenance requirements are affected significantly by the choice of architectural design and are an issue facing every designer.

As an example of some of the challenges associated with design of architectures, the reader is referred to the latest problems faced by the French in the design of their newest plant. "Development woes force EDF to abandon I&C System for N4," states *Nucleonics Week* of 3 January 1991 (Ref. 6.1). The latest design for French nuclear plants, the N4, is expected to carry the French nuclear industry into the leadership position in the use of computerized control rooms and man-machine interfaces. According to *Nucleonics Week,* the French utility Électricité de France (EDF) has decided to abandon the Controbloc P20. This is an architectural feature that includes a decentralized plant supervisory controller developed by the French supplier Cegelec. The article quotes an EDF official as saying that Cegelec had been having "major difficulties in perfecting the new product." The resulting delay in design of the I&C system will likely result in a delay to 1995 in fuel load at the newest French plant Chooz B1. Fuel load was originally scheduled for 1991, then pushed to late 1992 because of a voluntary stretch-out plus other general I&C problems in 1988.

A fallback system may have to be used in the N4. A change in architecture of the I&C system at this late date will impact the next four N4 plants, according to *Nucleonics Week.* This also could impact the use of the N4 control room concept, a cockpit design considered to be very helpful in improving operational

performance. The Cegelec system also was planned for the English Sizewell B plant. Cegelec was to provide all of the control system for Sizewell B, whereas it was providing only the lowest level of N4's I&C system (Ref. 6.2).

Scope of Study

For this chapter, the scope is limited to selected elements of the architecture of safety, control, and information systems. Not discussed are control room, auxiliary control room, and man-machine interface architectures. These subjects are discussed in other chapters of this report.

Most of the discussion concerns developments in France because, in the view of the panel, the French have the most advanced digital systems. There are briefer discussions of the German developments and Russian and Czechoslovakian work in I&C architecture.

NUCLEAR POWER PLANT I&C ARCHITECTURE IN FRANCE

The French nuclear industry has been very successful in the application of computer-based safety, control, and information systems. The architectures they have used are discussed here as examples of some of the best results to date in the application of digital technology to European nuclear power plants. The architectures have had to handle increasing amounts of information, as shown in Table 6.1.

Table 6.1
Amounts of Information Processed in French Power Plant Architectures

	Fessenheim	Creys-Malville	Chooz-B1
Starting Year	1970	1977	1984
Digital Entries	1500	8000	60000
Analog Entries	600	4000	2500
Graphic Images	-	500	17000
Volume in Mb/s	0.5	4	200

Upgrades on French 1300 MWe Plants

Électricité de France, the French NSSS engineering and construction company Framatome, and the I&C equipment manufacturers Merlin Gerin and Cegelec have acquired a great deal of experience in digital I&C systems over the past ten years. Cegelec provided a tabular summary of its efforts in I&C architecture in the French, British, and Belgian nuclear programs, shown as Table 6.2. According to Cegelec, there has been an evolution which has resulted in a system architecture being structured in layers of homogeneous processing, leading to a "durable" communication architecture (Ref. 6.3).

Micro-Z. Since Cattenom 1, which started in 1986, Cegelec's Micro-Z equipment has been used in 12 units of 1300 MWe, as shown Figure 6.3 and Table 6.3. The Micro-Z equipment uses self-contained cards, each of which includes up to 24 logic inputs; up to 8 analog inputs; up to 4 outputs for auto/manual stations; one microprocessor in charge of applications; one microprocessor that manages communication dialogue through two serial links; a set of RAM; and a set of EPROM memories containing the operating system, library, program written by the user, and the settings. Each card is equipped with a watchdog that detects failures and forces the auto/manual stations into manual mode when failures are detected. The Micro-Z card structure is shown in Figure 6.4 (Ref. 6.4).

Newest French Nuclear Plant I&C Architecture

The French are working hard to take advantage of lessons learned in the operation of their older nuclear power plants (Ref. 6.5). According to Framatome, its primary goals for I&C architecture are as shown in Table 6.4.

N4 I&C architecture. A new architecture has been designed to accomplish these goals in the newest French plant concept, N4. Construction of the first of the N4 plants, Chooz B, Unit 1, is nearly complete. Components of the N4 plant architecture are shown in Figure 6.5. The lowest level (Level 0) includes the sensors and actuators. The next level (Level 1) includes the automatic control and protection systems. It handles all automatic actions of the elementary systems and also performs automation of the wall synoptic diagram in the control room. It receives safety and protection manual commands directly from the control room and from the auxiliary panel. Level 1 receives from Level 2 all commands issued by the operator stations and transmits to Level 2 almost all of the information it acquires and processes. Level 2 handles installation control and operation tasks, processes information from a high synthesis level, and handles the interface with the operators. It has a centralized structure, with a centralization of information into a single database. Level 3 interfaces with technical management and maintenance functions. This highest level includes the computer-aided man-machine interface.

Table 6.2
Summary of the I&C Activities of the Cegelec Group in the French, British, and Belgian Nuclear Programs

	INTERLOCKS SEQUENCING ALARMS (1E)	CLOSED LOOP CONTROL	CONTROL ROOM SUPERVISION SYSTEM	REACTOR PROTECTION	NUMBERS OF UNITS
- FRENCH STANDARD 900 MW PWR PROGRAM (CP1 - CP2)	ELECTROMAGNETIC RELAYS	ANALOG ELECTRONICS '9020' SYSTEM	16 BITS DATA LOGGER BACKFITTED BY SAFETY PANEL (EDF DEVELOPED)	HARDWIRED ELECTRONICS (MERLIN GERIN)	32 UNITS
- FRENCH STANDARD 1300 MW PWR PROGRAM (P4)	MICROPROCESSOR BASED (8 BITS) CONTROBLOC N20	ANALOG ELECTRONICS '9020' SYSTEM	16 BITS DATA LOGGER BACKFITTED BY SAFETY PANEL (EDF DEVELOPED)	MICROPROCESSOR BASED (8 BITS) 'SPIN' (MERLIN GERIN)	8 UNITS
- FRENCH STANDARD 1300 MW PWR PROGRAM (P'4)	MICROPROCESSOR BASED (8 BITS) CONTROBLOC N20	MICROPROCESSOR BASED (8 BITS) "MICRO Z"	16 BITS DATA LOGGER BACKFITTED BY SAFETY PANEL (EDF DEVELOPED)	MICROPROCESSOR BASED (8 BITS) 'SPIN' (MERLIN GERIN)	12 UNITS
- FRENCH STANDARD 1450 MW PWR PROGRAM (N4)	MICROPROCESSOR AND DATA HIGHWAY BASED (32 BITS) CONTROBLOC P20	MICROPROCESSOR AND DATA HIGHWAY BASED (32 BITS) CONTROBLOC P20	32 BITS COMPUTER (GOULD) COMPUTERIZED CONTROL ROOM (EDF DEVELOPED)	MICROPROCESSOR BASED (32 BITS) 'C03' (MERLIN GERIN)	6 UNITS (2 IN CONSTRUCTION: CHOOZ B 1 & 2)
- BRITISH STANDARD 1100 MW NUCLEAR PROGRAM	MICROPROCESSOR AND DATA HIGHWAY BASED (32 BITS) CONTROBLOC P20	MICROPROCESSOR AND DATA HIGHWAY BASED (32 BITS) CONTROBLOC P20	DATA HIGHWAY AND VME 32 BITS BASED CENTRALOG P20	MICROPROCESSOR BASED (16 BITS) (WESTINGHOUSE)	4 UNITS (?) (1 IN CONSTRUCTION: SIZEWELL B)
- BELGIAN NUCLEAR PROGRAM DOEL 1 & 2 (BACKFITTED)	MICROPROCESSOR BASED (16 BITS) AC - 132	MICROPROCESSOR BASED (8 BITS) MRH 3000	16 BITS DATA LOGGER	MICROPROCESSOR BASED AC-132 AND MRH 3000	2 UNITS
OTHERS	MICROPROCESSOR BASED (8 BITS) MRH 3000	MICROPROCESSOR BASED (8 BITS) MRH 3000	16 BITS DATA LOGGER	MICROPROCESSOR BASED (8 BITS) MRH 3000	6 UNITS

MEANS \ SERIES	CP 1	CP 2	P 4	P' 4	N 4
START UP/SHUT DOWN CONTROLLERS	BINARY WIRED CONTROL		PROGRAMMED BINARY CONTROL		General Controller with Binary Processing Regulating Units
	U.C. (RELAYS)		CONTROBLOC		
SAFETY CONTROLLERS	ANALOG AND BINARY WIRED CONTROL		PROGRAMMED BINARY CONTROL		
	9020 + RELAYS		S.P.I.N.		Specific Digital Controller
REGULATING CONTROLLERS	ANALOG WIRED CONTROL			DIGITAL CONTROL	General Controller
	9020			MICRO Z	
DATA PROCESSING	COMPUTER		COMPUTERS		Computers with: - a control function - and several operators aid functions
	INFORMATION PROCESSING SYSTEM (1 LEVEL)		INFORMATION PROCESSING SYSTEM (2 LEVELS)		
REACTOR CONTROL AIDS			REACTOR CONTROL AID COMPUTER (FRA)		
DIAGNOSIS AIDS					
DISTURBANCES RECORDERS	TACHY	C A C E R + S. P. R. A. T.			Several Monitoring and Surveillance Systems
	CACER				
CONTROL ROOMS	1 MAIN CONSOLE 1 SECONDARY CONSOLE		1 CONSOLE ONLY		- 4 Operators Workstations with 3 graphic displays units 4 text displays units 1 minic actuated display
INSTRUMENTATION	STANDARD				

Figure 6.3. Evolution of Control Architecture in French Plants

Table 6.3
Milestones of the Digital Protection and Control Systems Design

1976: DECISION TO DEVELOP ENTIRELY NEW PROTECTION AND CONTROL SYSTEMS (FRENCH DESIGN BASES AND TECHNOLOGIES)

DIGITAL INTEGRATED PROTECTION SYSTEM	FREQUENCY CONTROL AND LOAD FOLLOW OPERATION	DIGITAL CONTROL SYSTEMS
	1976 ◆ MODE G DESIGN STUDIES	
1977 ◆ DIPS DESIGN STUDIES		
1978-80 ◆ MULTISECTION EXCORE CHAMBERS TESTED AT BUGEY 2	1979-80 ◆ FREQUENCY CONTROL OPERATION TESTED AT FESSENHEIM (MODE A) ◆ MODE X DESIGN STUDIES	1980-82 ◆ CONTROL SYSTEMS ADAPTED TO GRID REQUIREMENTS
1981 ◆ LINEAR POWER DENSITY AND DNBR CALCULATION MOCK-UP TESTED IN BASE LOAD OPERATION AT TRICASTIN 3	1982 ◆ DECISION TO OPERATE THE 1500 MW UNITS WITH THE MODE X	1982 ◆ DESIGN OF DIGITAL SYSTEMS TO BE INSTALLED ON ALL 12 MOST RECENT 1300 MW UNITS STARTING WITH CATTENOM 1
1981-83 ◆ MOCK-UP TESTED DURING LOAD FOLLOW AND FREQUENCY CONTROL AT TRICASTIN 3	1981-83 ◆ MODE G TESTED AT TRICASTIN 3	
	1983 ◆ MODE G LICENSED ◆ MODE G IMPLEMENTED ON PLANTS (TRICASTIN 2, CHINON 1)	
1984 ◆ DESIGN STUDIES OF AN ADVANCED DIPS FOR THE 1500 MW UNITS ◆ PALUEL 1 CONNECTED TO THE GRID	SINCE 1983 ◆ MODE G IMPLEMENTED ON ALL 900-1300 MW UNITS (WITH THE EXCEPTION OF FESSENHEIM BUGEY)	1986 ◆ CATTENOM 1 CONNECTED TO THE GRID
	1990 ◆ St ALBAN 2 EQUIPPED WITH A PROTOTYPE ENABLING BOTH MODE G AND MODE X ◆ MODE X TESTS IN APRIL 1990	
TODAY: 50 REACTOR-YEARS OPERATING EXPERIENCE	TODAY: ALL UNITS MEETING FULL GRID REQUIREMENTS	TODAY: 15 REACTOR-YEARS OPERATING EXPERIENCE

SPIN and DIPS are respectively French and English names:
Systeme de Protection Integre Numerique
Digital Integrated Protection System

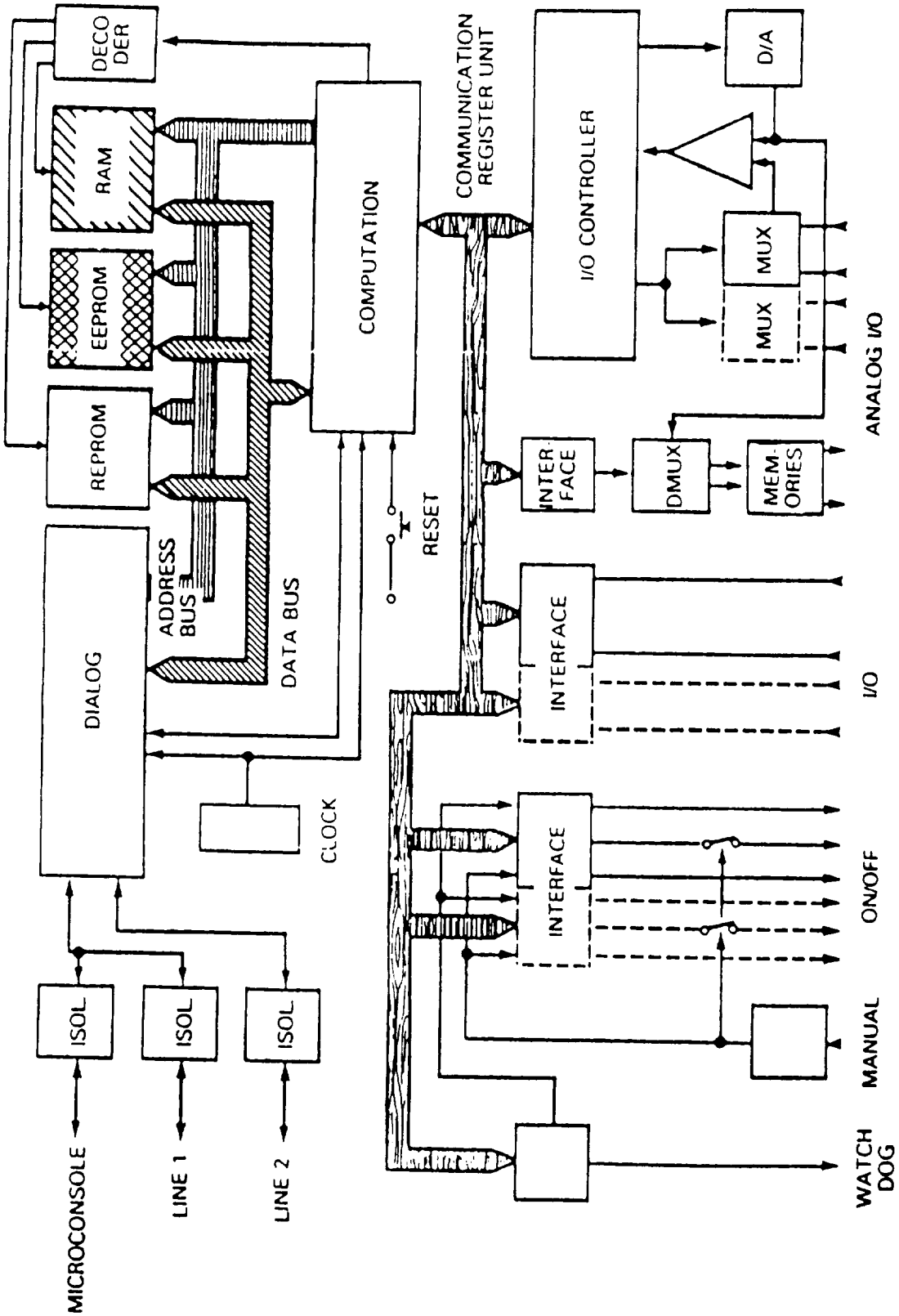


Figure 6.4. Micro-Z Card Structure

Table 6.4
Lessons Learned in French Nuclear Power Plant I&C Architecture

	Goal	Approach
1.	Eliminate effects of I&C failures	Redundancy
2.	Increase reliability	Local area networks; new technology to eliminate connectors, relays, etc.
3.	Increase computational capability	Modern microprocessors
4.	Simplify interfaces	Local area networks

As Figure 6.5 shows, there are two subsystems in Level 1: the reactor protection and control system (CO3) manufactured by Merlin Gerin, and the logic and control system (P20 Controbloc) manufactured by Cegelec.

CO3 system. The CO3 system has as its main function core protection and control. It has three subsystems. The first subsystem is the rod control subsystem (RGL). This subsystem regulates the core in three possible modes, similar to its Westinghouse counterpart. The second subsystem is the core protection subsystem (RPN), which takes information from the nuclear flux detectors and other sensors. The RPN includes a class 1E portion that provides signals to the protection system, and a nonsafety portion that supplies signals to the control system and a surveillance system described below. The third subsystem is the reactor protection system, "Système de Protection Intègre Numérique" (SPIN).

Protection System Upgrade for French Plants--SPIN

The French decided in 1976 to develop an entirely new protection system to improve the operating margins and safety levels of their 1300 MWe plants. The use of digital technology was approved by the French safety authorities because an enhanced safety level could be demonstrated analytically. This is the SPIN design. Merlin Gerin in France was chosen as the manufacturer.

There are four protection channels powered by two electrical trains. Every accident must be detected by two different protection functions, which will be implemented in different functional units. There is one ex-core neutron detector

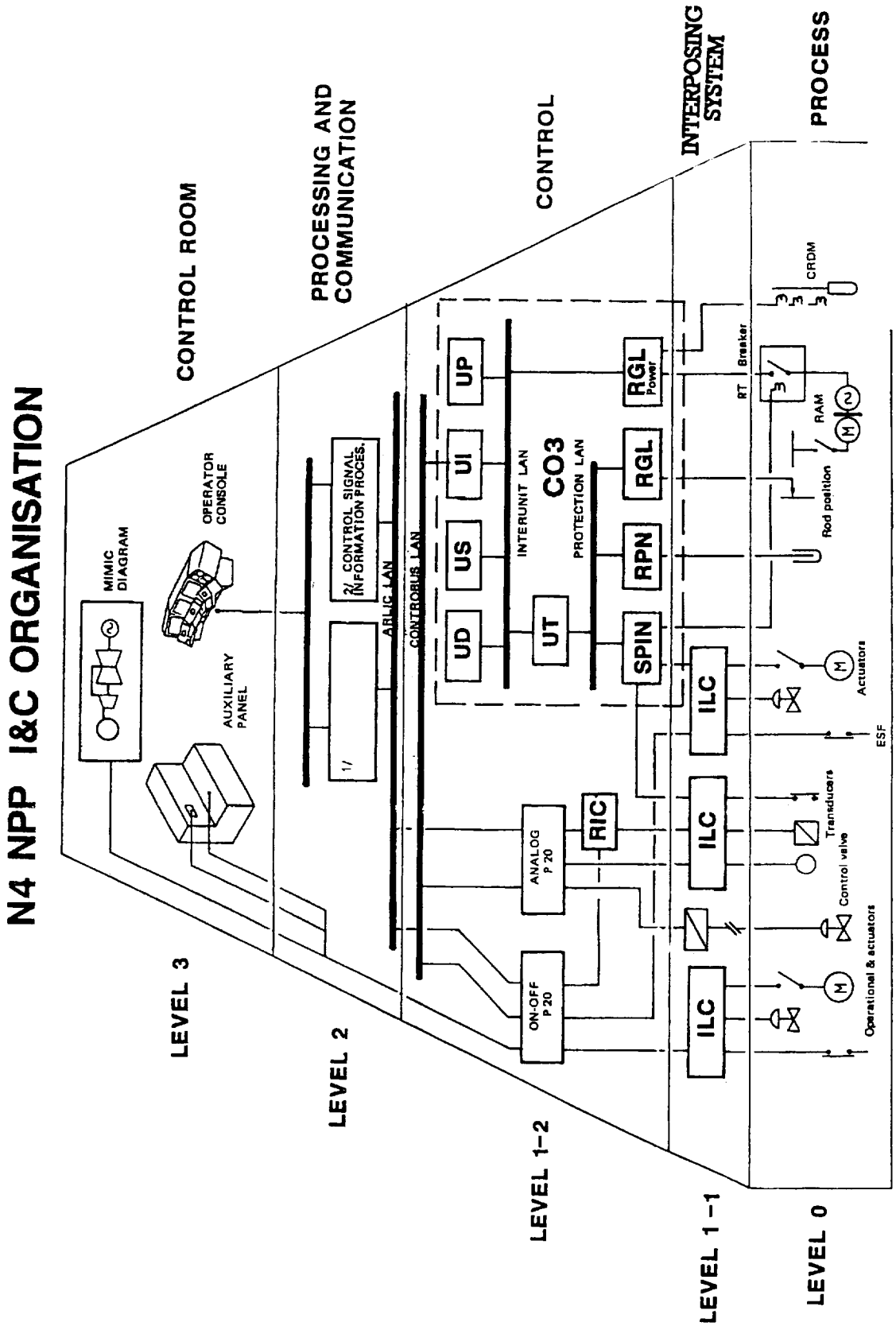


Figure 6.5. N4 NPP I&C Organization

with six channels in each quarter of the core, as shown in Figure 6.6. According to Framatome, the approach is very similar to the Combustion Engineering core protection calculator (4 levels) of the early 1980's. FRAMATOME, Merlin Gerin and Electricite de France decided to develop a more modern version of the SPIN. This version is being installed in 1500 MWe units. There are two local area networks (LANs) in each channel, for a total of eight LANs. The eight protection LANs are transformed to optical for improving data transfer rates and providing electrical insulation. The LAN speed is approximately 2.5 Mb/s. Fiber optics give more band width. Some U.S. hardware and software are used. There is generalized use of 2/4 logic, with graceful degradation to 2/3 and to 1/2, when one channel is failing or undergoing periodic tests.

SPIN acquires significant measurements, makes calculations in real time, compares with thresholds, and finally, drives emergency shutdown and safeguard actions. These complex processes require the cooperation of several processors working in parallel. The modification to the older protection system consisted of adding four data acquisition and processing units and two core monitoring units as shown in Figure 6.7. The System of Process Instrumentation (SIP) ensembles are implanted in four redundant and physically independent units, each of which is connected to four process units of the protection system. Each Acquisition and Processing Unit for Protection (UATP) is an ensemble of two acquisition units and five functional units (UF). Each functional unit is built around a Motorola 68000 microprocessor. The hardware is Motorola 68000, 68881-based, with a speed of 10 MHz. A faster version is available with a speed of about 16 MHz. Stations connected to networks use a deterministic protocol. Every station is authorized to speak only when it has received a token. This is done in a cyclic manner, in which cycle time is constant.

Cabling in the SPIN system is coaxial or optical when decoupling is needed. The communication is 2.5 Mb/s, with a margin of 50-60%. All equipment is 1E qualified. Compliance with IEC 880 and U.S. DOD 2167 standards limited the use of interrupts.

SPIN develops PPS logic from the RGL and the RPN inputs, provides diagnostics and monitoring, and provides an operator interface. The entire protection system is 1E qualified. The SPIN-P4 has accumulated five years of use at twenty units. SPIN has approximately 40,000 lines of assembly code. The P-4 version of SPIN software was developed in the 1980-84 time frame. There have been nine successive software versions.

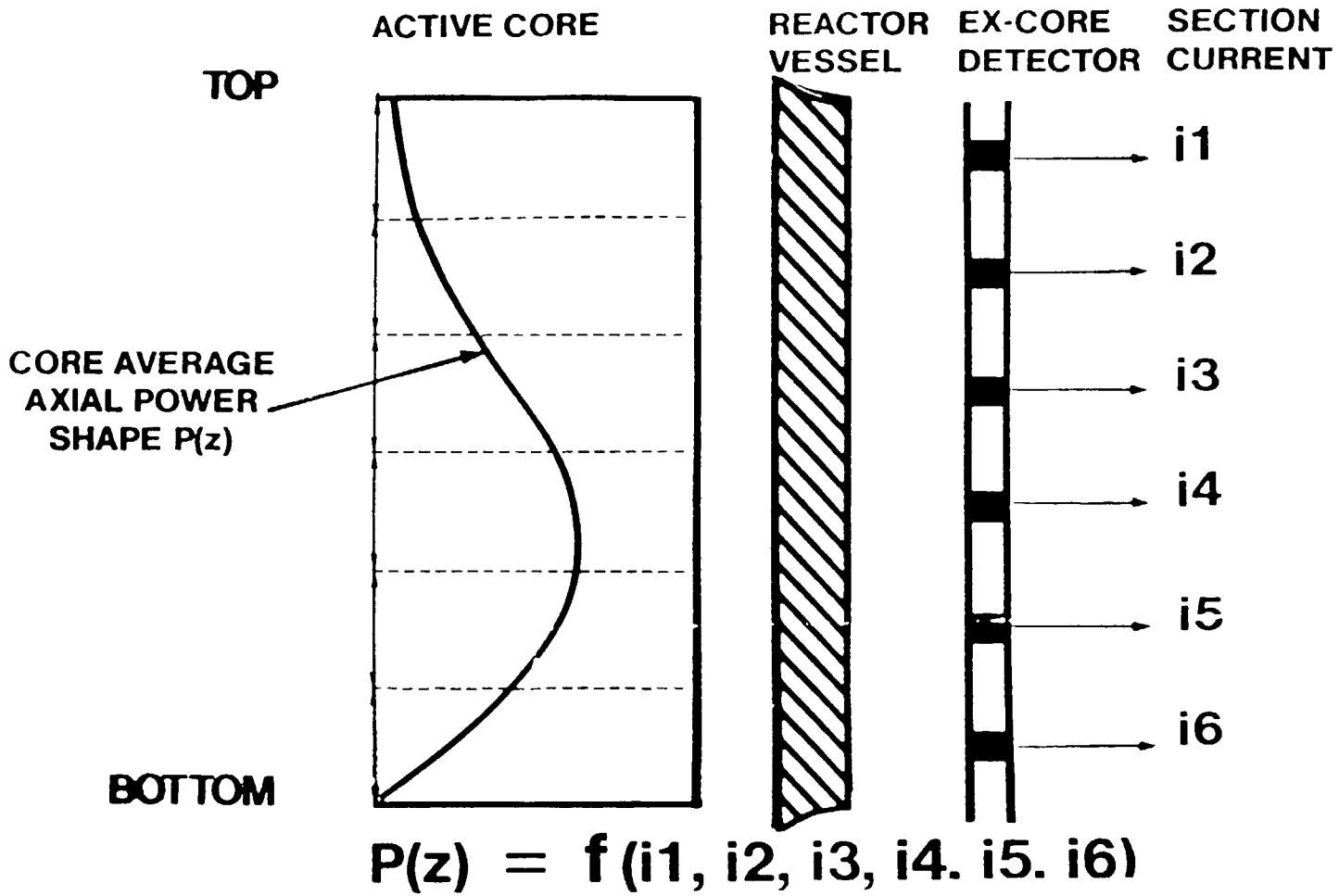


Figure 6.6. Measurement of Axial Power Distribution

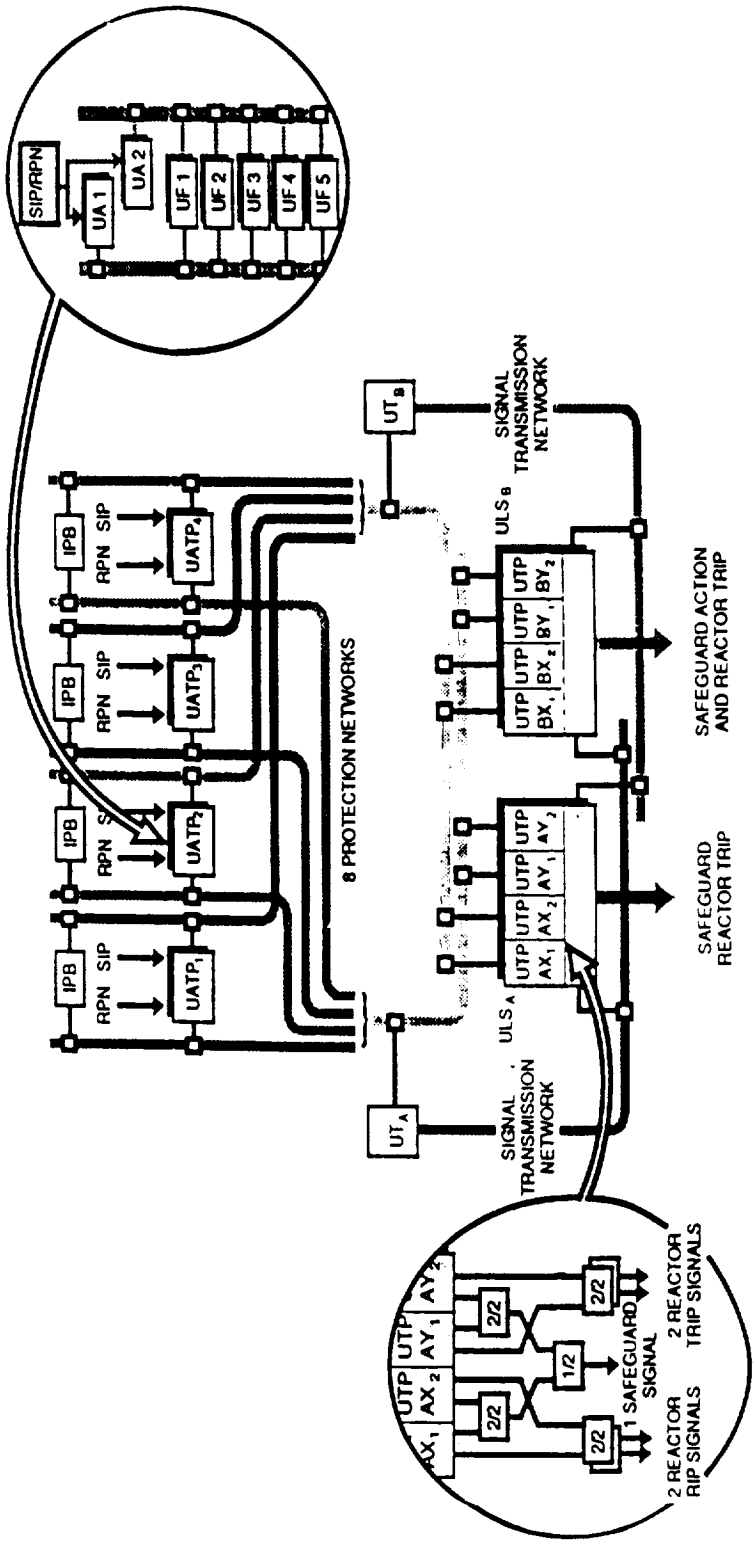


Figure 6.7. Organization of the SPIN

Newest French Control System Architecture--P20 CONTROBLOC

The newest control system concept and design is Cegelec's P20 Controbloc equipment. The P20 is organized around a redundant serial local area network (LAN). It is designed to be an improved version of Cegelec N20 equipment. The major difference is in the sophisticated hardware: the P20 uses modern 16/32-bit microprocessors and transputers, while the N20 uses 8-bit machines. (The N20 system was developed from 1978-1988. Its main advances over older Cegelec equipment were self-testing, improved control room, and fewer annunciators. This system replaced relays with 8-bit microprocessors.)

The P20 was designed for higher availability and reliability. It uses extensive self-checking and dual redundancy. Use of high-level programming languages (C for microprocessors, Occam for transputers) will allow easier useability. A high-speed data highway of 2.5 Mb/s is used. A traffic manager is used to provide a deterministic system. 1E is separated from non-1E by optic fiber. Datalinks provide communication with other systems. Intercluster controls are used to provide synchronization. CRTs are used for maintenance and testing. In one cubicle, there may be 1000 inputs/outputs. Terminals are provided on backplanes.

The software common mode failure requirement is addressed in the P20 by functional diversity. Application software is separated from system software. The French are moving to ADA for specification; at present, ADA is used in the control room only. Software costs were estimated to be partitioned as follows: 50-60% for test phase, 30% for software specification, and 10% for coding.

NUCLEAR POWER PLANT I&C ARCHITECTURE IN GERMANY

According to the Siemens-KWU personnel with whom the panel met, there has been a special combination of factors in the German nuclear industry which has allowed the Germans to be very successful to date in their plants. Five factors are (1) turnkey contracts, (2) common rule making, (3) high automation level of conventional power plants, (4) very low turnover of operations staff, and (5) requirement from the start of the nuclear program for full load following. Due to these factors, a great deal of empirical knowledge has been factored into German designs, and lessons learned throughout the nuclear industry have resulted in positive changes in all of the German plants.

Limitation System. Out of this unique environment has grown a unique element of nuclear plant I&C architecture, the "Limitation System." This system fits between the normal control system and the normal safety system known to U.S. designers. The functions of the limitation system are to: 1) automatically minimize the number of scrams; 2) minimize stress to the big mechanical components by smoothing most transients; and 3) give more time to operators for information gathering and

diagnosis. Although this system has been described several times in the literature and has been very successful, there is very little discussion of it in the United States. According to Mr. Werner Aleite of Siemens-KWU, this system grew out of unique requirements in Germany for full load following and for rapid recovery from operational upsets (Ref. 6.6). This limitation system was control system grade in the Biblis type reactors. Since Grafenrheinfeld, it became protection grade. Now the limitation system is the biggest I&C system in German nuclear power plants.

The latest I&C design in a German plant can be found at Isar-II, operating for more than one year. As is the case for France, the number of signals fed to the control room has grown dramatically, as shown in Fig. 6.8 (Ref. 6.7). Brokdorf, commissioned in 1986, had 2000 analog and 13000 binary signals (Ref. 6.8).

The German reactor protection system is of analog design but has used digital (pulsed) signals to detect and announce failures. The Germans have used this type of system for 20 years. They also have used it generally for other protection systems besides the reactor protection systems. Eventually, Siemens-KWU is going to digital protection systems; a digital safety system is under development now. Interesting features include use of TCP/IP, ethernet, and optic cables in some places. There will be no token; the system will be deterministic by cyclic communication and there will be no main bus. To improve reliability, there will be a free repair channel. Effectively, this provides 2/4 logic. There will be ring storage of the last 2000 values.

In discussions with the Siemens-KWU personnel, panelists were impressed by the amount of knowledge which they had about the architectures of the U.S. designs and the designs of other countries. There were a lot of references to Westinghouse, Combustion Engineering, General Electric, and Babcock & Wilcox designs. The requirements developed by the Electric Power Research Institute (EPRI) for the next nuclear plants to be built in the United States are considered seriously in the design of German plants. In these discussions, for example, the panel learned that the new Siemens-KWU protection system is envisioned to be like that in the British plant, Sizewell B. Our hosts indicated that the Sizewell B requirements were very similar to what KWU has learned from its experience.

Information System Architecture for Siemens-KWU Plants--PRISCA

A very interesting information system seen by the panel was the PRISCA, a computer-aided process information system (Ref. 6.9 and 6.10). Computers have been used in German plants for many years, but this system is the most advanced use of computers to date. The PRISCA system is used as an additional system to get personnel acquainted with the plant. The operator does not need PRISCA to operate the plant safely.

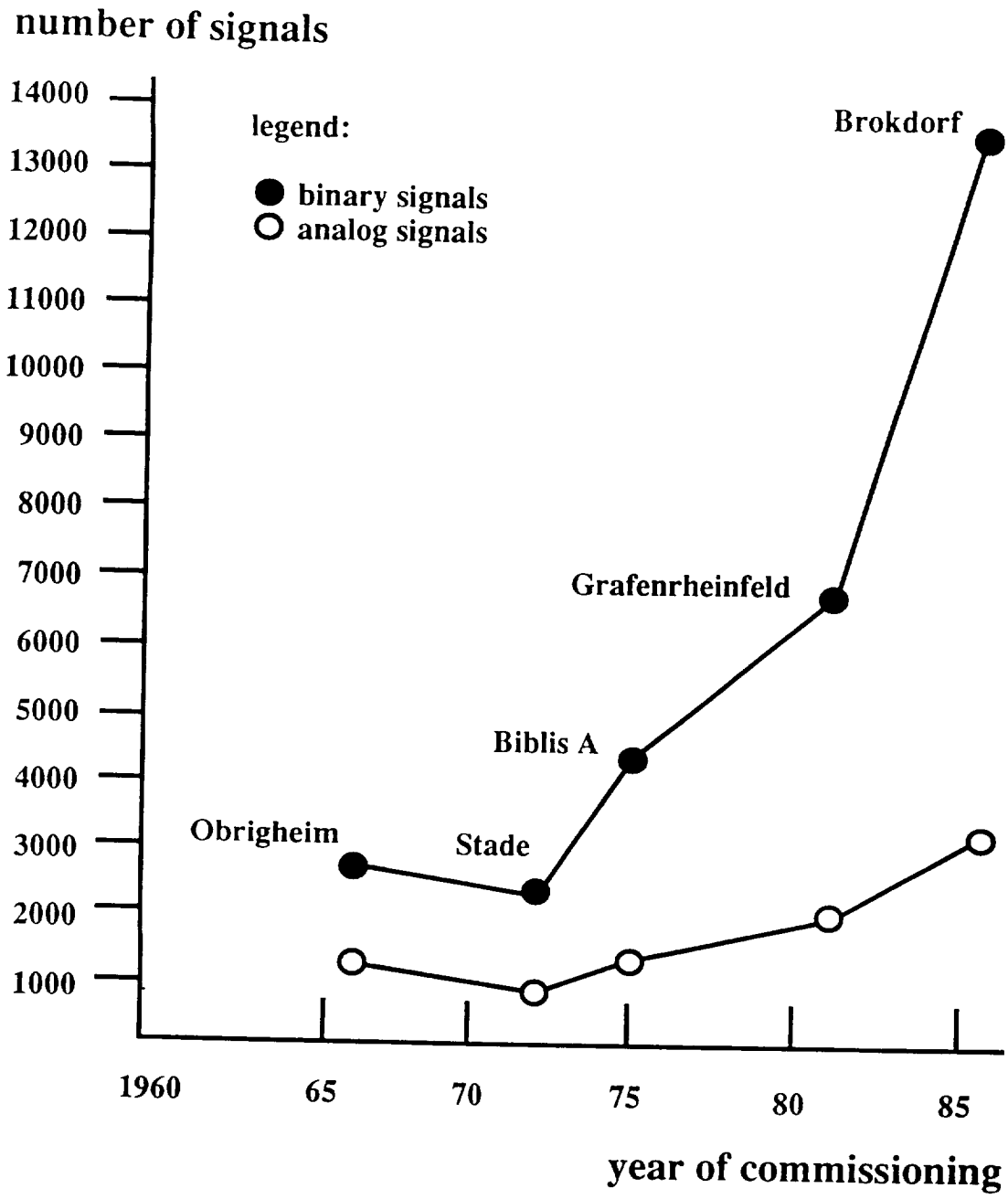


Fig. 6.8. Increasing number of signals fed to the control room in German nuclear power plants.

PRISCA's main functions are shown in Figure 6.9 (Ref. 6.11). This system integrates functional connections from plant processes and I&C systems in addition to performing most conventional functions like alarm annunciation, nuclear computation, and log printing. (An example of a PRISCA overview display is shown in Chapter 5.) The PRISCA design is already in operation in six KWU plants. This system is different from other information systems seen by the panel with respect to the output formats, which require a great deal of data synthesis. The hierarchic architecture of the I&C system is shown in Figure 6.10. Redundant communication buses independently connect the automation devices to the process information system PRISCA and the operating processor system for manual control. Priority drive control modules process the signals from the I&C safety modules. A separate interaction line for manual control via conventional desk tiles is provided for safety system components.

NUCLEAR POWER PLANT I&C ARCHITECTURE IN THE SOVIET UNION

A lot of activity is present in the U.S.S.R. in the design of I&C for nuclear power plants. Especially since the Chernobyl incident, the nuclear industry is very aggressive in the development of improved systems to prevent operator error, to improve the ability of the safety and control systems to survive operator error, and to improve safety margins. Many results are still of the pilot type since new plants are not being ordered. At the workshop on Instrumentation and Control held in Washington, D.C., Mr. Rakitin of the I.V. Kurchatov Institute of Atomic Energy, Moscow, indicated that a significant capability for simulation of the performance of I&C is being developed. The Kurchatov Institute feels that simulation of I&C is essential to the verification and validation of design before construction.

A very important program in the U.S.S.R. is the modernization of existing systems. On several occasions, the panel was told of the need to upgrade I&C to improve safety related aspects in the near future (Ref. 6.12). The nuclear community, worldwide will be very interested in how the Soviet go about this upgrade.

For new designs, high goals are being set. The Soviets are designing a conceptual I&C system with a failure rate goal (for core melt) of 10E-9 for the 1E functions and 10E-1 or -2 for auxiliaries and noncritical functions. Some components must survive earthquakes of 3 to 8 on the Richter scale. As is the case in all other designs, significant use of functional diversity is planned. This system may be much more expensive than the current 20-25% of cost of plant. The main features of the system are under development now. There is a main local net. Local area networks include programmable logic controllers, actuators, and sensors. To get high reliability, Soviet designers are considering triple modular redundancy, 2/4 logic, and built-in diagnostics.

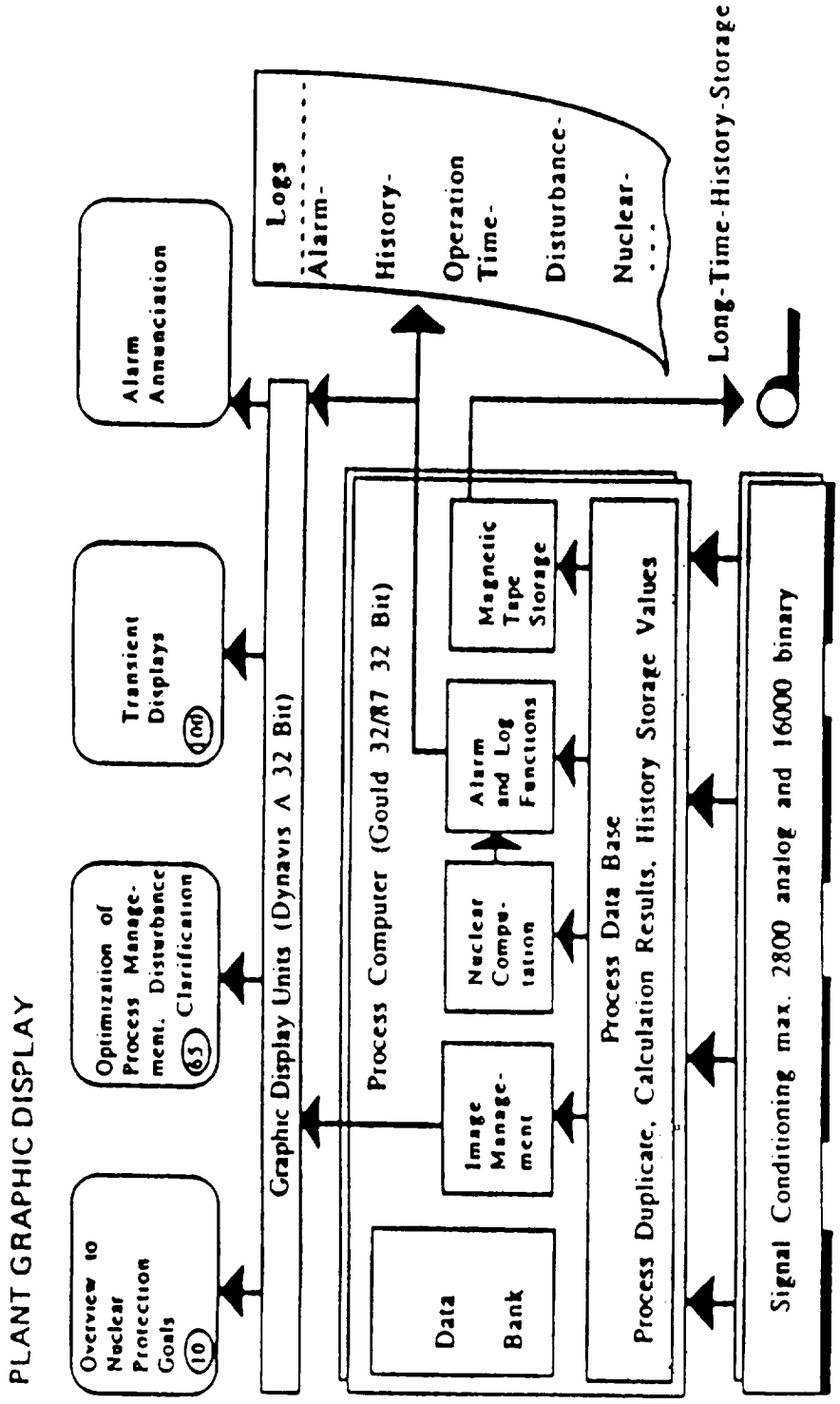


Figure 6.9. PRISCA (Process Information System, Computer-Aided) Main Functions

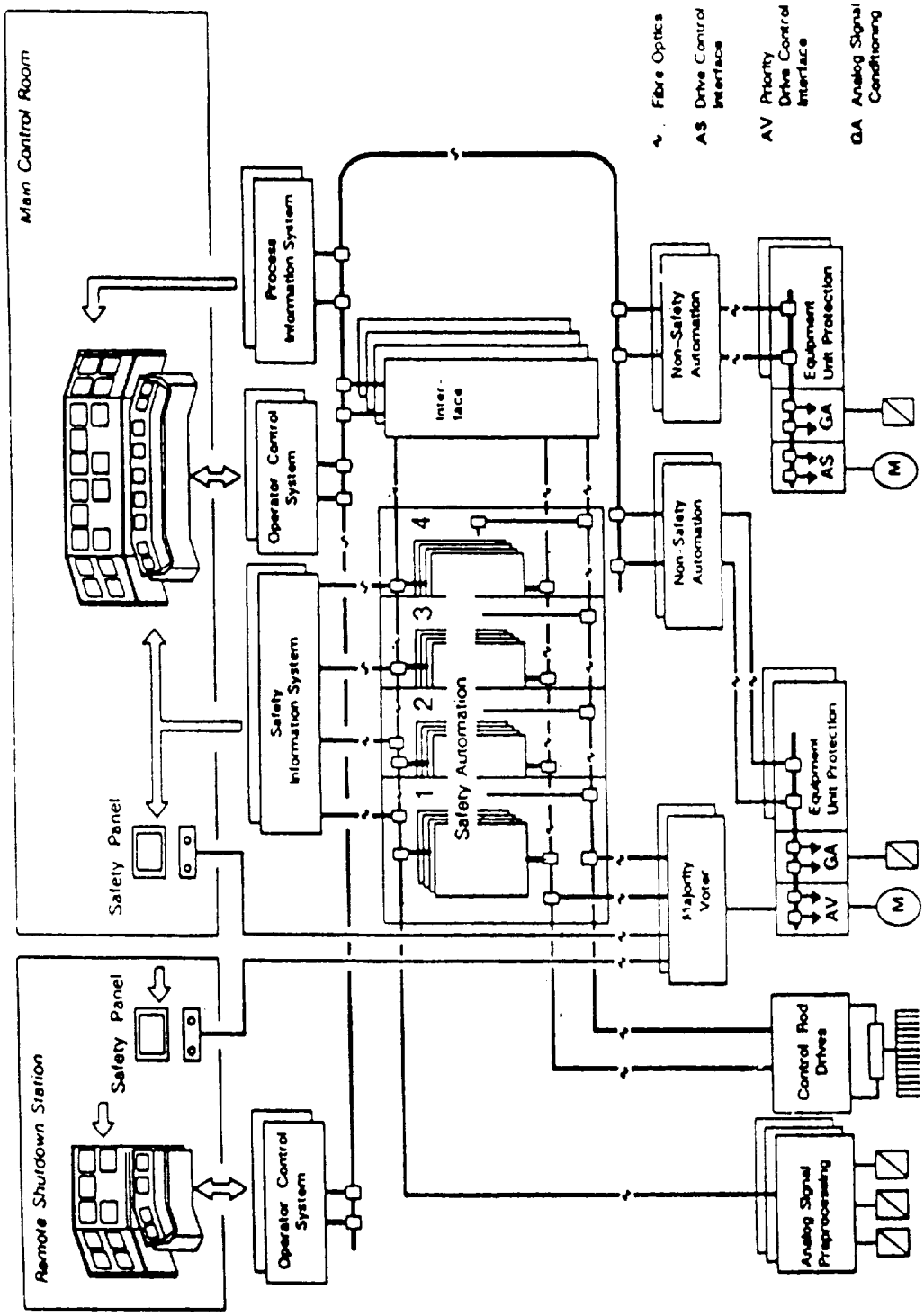


Figure 6.10. Overall Structure of I & C System in a Nuclear Power Plant

After Chernobyl, there is an emphasis on the unreliability of the human operator. However, at present, there is in the control room about 10 Mbit of information presented to the operators, and in accident situations, the operators may have little time for decisions. Because of these considerations, operator support systems are considered a very high priority. Some of the technological possibilities envisioned by scientists are still difficult to implement in the U.S.S.R. because of limitations in computing power at the nuclear plants. This is especially true for upper levels of the I&C hierarchy, where a great deal of information needs to be integrated and presented to the operators or the systems that would replace some of their functions.

The main problem, according to our Soviet hosts, is the need for very powerful computers, ones with a capability of 10 million operations per second and with high external memory. The nuclear industry in the Soviet Union does not at this time have access to this capacity. (At present, designers believe they can implement lower level requirements easily.) Soviet I&C designers are laboring with inadequate computer resources. While in the United States we are using 32-bit Gould SEL machines along with newly emerging pixel graphic display generators, the Soviets are trying to build full-scope simulators (5000 equations) and sophisticated graphics with PCs of the IBM-XT generation (it seems) and character graphics display generators.

Several Soviet organizations are working on I&C for nuclear plants. The Leningrad Atomic Energy Institute designed the I&C for the Finnish Loviisa power plant. Design implementation included some Siemens equipment. Other organizations in Leningrad are also working on new I&C. The latest defense achievements, if promising, are being examined for application to nuclear power plants.

Another organization working on I&C is the All-Union Institute of Electrical Mechanics, VNIIEM. Interestingly, this institute reports to the Ministry of Electromechanical Engineering, not the Ministry of Atomic Energy. Its main concern is satellites, but it has experience in computer and control systems in manufacturing, metallurgical processes, and nuclear energy. Because of its demonstrated capabilities in several fields, it has been given responsibility for (1) development and integration of the control system for RBMK plants, and (2) the control and protection system for VVER plants.

An example of Soviet I&C architecture is the Skala for RBMK installed in 1971 in the Leningrad power plant; VNIIEM developed the plant's information system. The system has 11000 control points with a period of control of one minute. This reactor type has 2000 channels; it is necessary to monitor flux distributions in each of these and to represent this information to the operating staff. An expanded system will be operational in two to three years. The ultimate objective is control operation of 5s with improved information supplied to the operation staff. The plan

is to connect to the old, obsolete computer system a multibus system based on the microprocessor INTEL 8086 or 8087.

Some of the problems in existing plants are related to the slow rate of monitoring and registration. Others are related to new safety requirements introducing new computational functions. The 1960s machines in use cannot perform satisfactorily, particularly in transients. Furthermore, the system is aging and the Soviets are worried that there may be a reliability cliff not far away from their present position. As in most countries, complicated algorithms requiring complicated or expanded architectural features are tried first in information systems, whose speed of response and performance are not strong direct factors in safety (Ref. 6.13). Other problems of concern in the Soviet plants are associated with cable aging (Ref. 6.14). The U.S.S.R.'s Research and Development Institute of Power Engineering is working on this problem. This is also a significant concern in the United States; EPRI is working on this problem.

NUCLEAR POWER PLANT I&C ARCHITECTURE IN CZECHOSLOVAKIA

There are eight VVER units operating in two Czechoslovak plants. These are of the Russian 213 type (more advanced safety features than the 230 type). An additional four units are under construction for a third plant site. These plants use Soviet technology for safety and control, and Czechoslovak technology for the control system of the non-nuclear part of the plant (which produces steam). At present, these plants use only hard-wired systems, not computer-based systems. In recent agreements with KWU, the German Konvoi I&C system will be used for upgrade of I&C at the Mochovice-1 and -2 plants, both model V-213s (Ref. 6.15). The safety system will remain Soviet and will be essentially type 213 hybrid system logic rather than digital so that the plants retain their fuel warranties. The turbine control system will be of Skoda design.

SUMMARY OF ARCHITECTURE STUDY

1. Activity in R&D, design, and implementation of new I&C architectures is a little more intense in Europe than in the United States, due to the real-life problems being faced there now. The French were facing tough issues in deciding whether to qualify the P20 Cegelec design for Chooz-B1 or to use an older well-proven architecture. The Germans are trying to digitize the noncomputer-based enlarged intelligent protection system that has functioned well for several years in their plants. The Soviets are undertaking significant development efforts to utilize computer-based architectures to improve their plants. The Czechoslovaks are looking harder at non-Soviet technology to see if there exist products that can significantly improve their nation's plants.

2. Designers of new concepts are trying to rely only on technology already proven. All countries are moving to digital technologies, but only deterministic architectures and classical algorithmic approaches are being incorporated. Whereas in the United States fossil plant technology is being proposed for nuclear plants, the Europeans are a little more aggressive. The West Europeans are planning to include fossil and industrial experience. In the U.S.S.R., defense technology is being looked at for possible application to nuclear power. These countries do not seem to be considering very advanced networks (optical); this is also the case for U.S. designers. No triple modular redundant (TMR) systems were discussed, but some are used in United States.

3. Europeans seem very aware of U.S. nuclear technology. Their past architectures have been patterned after U.S. designs, except for the German Limitation System, which seems to be totally different in philosophy as well as application.

4. New concepts are not relying as much on U.S. nuclear industry, although the DOE/EPRI ALWR Requirements Document was mentioned in several of our meetings. The impact of the U.S. computer technology, however, is undeniable. Almost all of the designs include U.S. computer hardware technology.

5. Standards development in Europe is not keeping up with technology advances in architectures (existing or planned). This is also the case in the United States; however, the Europeans seem to be working harder in this area. Europe is moving toward use of standard off-the-shelf components.

6. The German Limitation Control System adds another layer to power plant architecture. This seems to be a unique development of intelligent control. Although it has been implemented using analog technology, the system logical architecture seems advanced compared to other U.S. and European designs. The U.S. nuclear community is relatively unaware of this development.

REFERENCES

1. MacLachlan, A. "Development Woes Force EDF to Abandon I&C System for N4." *Nucleonics Week* (3 January 1991).

2. MacLachlan, A. "British Support French I&C System that EDF has Abandoned for Its N4." *Nucleonics Week* (10 January 1991).

3. Combe, M. "Evolution of Operating System for Electronuclear Power Plants at EDF." Personal communication, 28 November 1990.

4. Mourlevat, J. L., A. Parry, et al. "Instrumentation and Control Revamping." *Fission Reactors* (13 March 1990).

5. Parry, A. "Nuclear Power Plant I&C: A Modern Concept."

6. Aleite, W. "Leittechnik Systems in Nuclear Power Plants and Their Importance to Reactor Safety." *Atomkernenergie Kerntechnik* 45 (4):219-229 (1984).

7. Bastl, W. Personal communication, GRS Garching, November 30, 1990.

8. Hoffman, H., H. D. Fischer, K. H. Lochner, U. Mertens. "Digital Information and Control Systems" Paper presented at the Poster Session during the European Nuclear Conference in Lyon, France, 23-28 Sept. 1990.

9. Aleite, W., K.H. Geyer, "Safety Parameer Display System Functions on Integrated Parts of the KWU KONVOI Process Information System" Fifth International Meeting on Thermal Nuclear Reactor Safety, Proceedings Vol. Z, KfK 388012, December 1984.

10. Aleite, W. "Operator Support by KWU KONVOI PRINS." International Conference on Modern Power Stations, Liege, October 7-11, 1985.

11. Bock, H-W. "Future Main Control Room Design for Siemens Nuclear Power Plants." IAEA-CN-49/28.

12. Malkin, S.D. "NPP Automatization Concepts and Problems." Preprint IAE N4835/4, Moscow, 1989.

13. Adamov, E. O., P. A. Gavrilov, A. I. Gorelov, A. I. Ephanov, M. N. Michailov, and N. A. Sazonov. "An Automated Data System for the Monitoring of RBMK-1500 Reactors: Status and Potential." IAEA-CN-49/98.

14. Kondratiev, V. V., and V. K. Prozorov. "Effect of I&C Cable Ageing on Nuclear Reactor Safety."

15. "Siemens-KWU Picked for Mohovice I&C Replacement." *Nucleonics Week* 31 (no. 41, 11 October 1990).

CHAPTER 7

INSTRUMENTATION

Frederick R. Best

INTRODUCTION

The panel's objective in reviewing European nuclear power plant instrumentation was to discover devices, approaches, or phenomenology that could be usefully employed in the U.S. nuclear power industry, particularly in light water reactor (LWR) plants. In order to achieve this objective, the panel first searched the literature to identify individuals and organizations carrying out research pertinent to the objective. Site visits were then arranged within available time constraints so that state-of-the-art information could be gathered.

This chapter summarizes the instrumentation information collected from site visits and the literature; evaluates the technology relative to that in the United States; and indicates which areas may be of interest to the United States. The technologies of France, Germany, and the Soviet Union are described, and these are compared to technologies in the United States. Nuclear instruments and then temperature, pressure, flow, and other devices are discussed for each country. Throughout this chapter, the major emphasis is on instrumentation that is in commercial service or has been tested in-reactor, except for devices that seem to have exceptional potential for enhanced performance.

FRENCH INSTRUMENTATION

The French PWR industry is founded on the Westinghouse plant design, but there are significant evolutionary improvements.

Nuclear Detectors

The N4 plant design operates with six axial section, ex-core power detectors for both overall power level and axial power distribution determination. These

detectors operate in conjunction with the rod control system to provide three progressively more complex plant operating modes culminating in Mode X--the simultaneous temperature and axial power offset control.

Advanced cores are being designed with reduced neutron leakage to mitigate the reactor vessel embrittlement problem. However, this also reduces the flux at the ex-core detectors, which has impelled the French to develop improved in-core detectors. Ten sets of nine-chamber, in-core detectors are to be tested in an Électricité de France (EDF) power reactor in late 1991. These detectors use gallium arsenide electronics in containment, near the vessel to multiplex the signals and reduce containment cabling and penetrations. Fiber optics are used as optical isolators, not for increased bandwidth.

A variety of miniaturized in-core fission chambers have been developed and tested. Table 7.1 (Ref. 7.1) lists the principal characteristics of these detectors.

Table 7.1
French Fission Chamber Characteristics

Name	CFUZ 53R	CFUZ 43	Prototype
Sensor	90% U235	90% U235	90% U235
Fill Gas, Argon (kPa)	800	110	250 (+N_2)
Insulators	Alumina	Alumina	Alumina
Location	In-core	In-core	In-core
Geometry			
Diameter (mm)	1.5	3	not available
Length (mm)	10	13	not available
Sensitivity $\frac{A^2/V^2}{N/cm^2\text{-}S}$	$3x10^{-20}$	$3x10^{-18}$	not available
Range $N/cm^2\text{-}S$	$1x10^{12}$-$1x10^{14}$	$1x10^{11}$-$1x10^{14}$	$1x10^{0}$-$1x10^{11}$
Max Operating Temp. (°C)	350	350	not available

Figure 7.1 is a photograph of the CFUZ 53R detector. Figure 7.2 is a schematic of the detector internals together with two other more conventional detectors. Note that this detector is only 1.5 mm in diameter.

In addition to the above detector, a prototype fission chamber capable of eleven decades of neutron response is being fabricated for the REP 2000 and for backfitting in older plants. This detector has multiple internal electrodes: one large for source range sensitivity, and two other, smaller electrodes for the intermediate and power ranges. This one detector is to replace three separate detectors.

Temperature and Pressure Sensors

No new temperature or pressure sensor technologies are being developed for reactors through the N4 plant (Ref. 7.2).

Figure 7.1. CFUZ 53R Detector

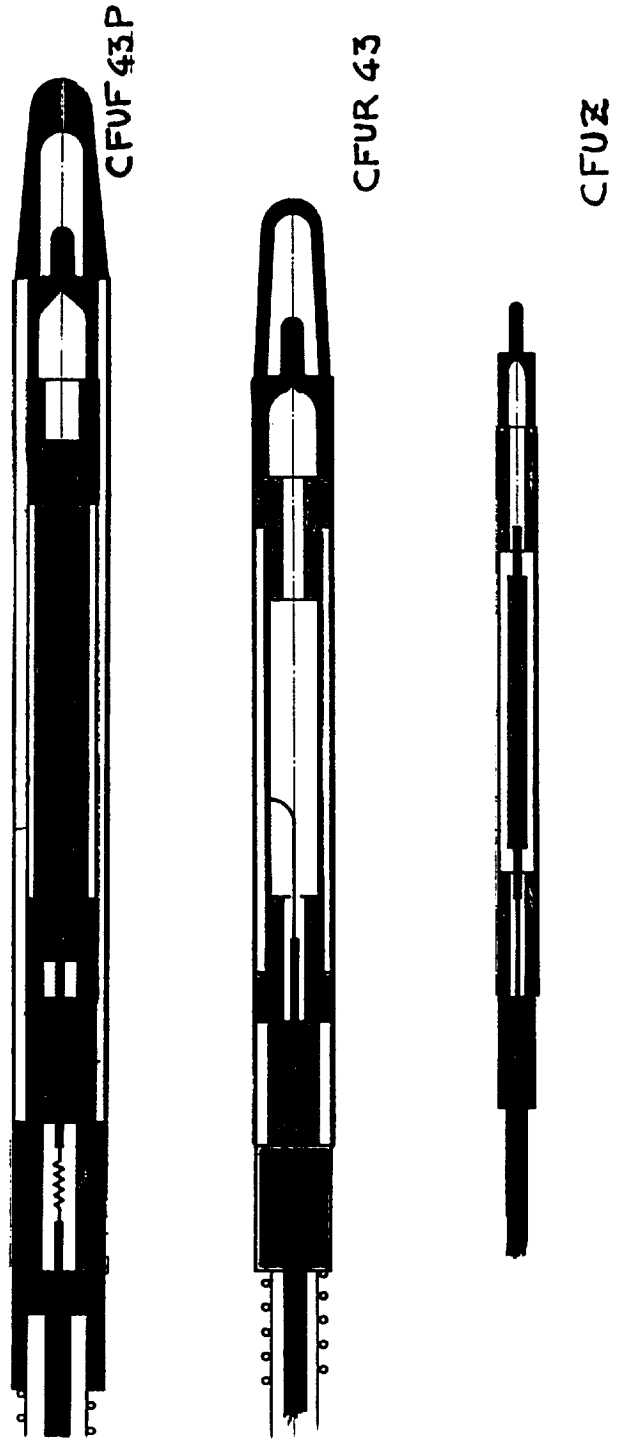


Figure 7.2. Comparison of Internals of 3 Detectors

Other Sensor Technologies

Fiber-optic networks are being considered for in-containment instrumentation systems. Breuzè (Ref. 7.3) has carried out experiments for reactor instrumentation systems, showing that silica fibers can sustain 600 Gy of gamma dose and function properly for links hundreds of meters in length.

The French electrical power grid is so highly dependent on nuclear generated capacity (>70%) that load following with nuclear plants is required. Tallec (Ref. 7.4) has developed control algorithms that synthesize core exit thermocouple and ex-core neutron power readings to simultaneously control core average temperature, axial power offset, and coolant enthalpy rise. Leroy (Ref. 7.5) has demonstrated that a PWR can simultaneously load follow and maintain optimum power distributions without boron concentration changes by the use of "gray" and black control rods. In both systems, plant measurements are compared with a three-dimensional power distribution computed in real time. Optimal rod positions are computed using a statistical minimization technique called "simulated annealing" where the core may continuously be burned most efficiently in a way an operator could not duplicate simply by control room indications.

GERMAN INSTRUMENTATION

Felkel (Ref. 7.6) has noted that the German PWR industry has not found sensor technology to be limiting as to plant operation or design and that there is no fundamental sensor technology development program. Nevertheless, sensors developed and proven in other industries (e.g., aeronautical, chemical, medical) may be adapted for the nuclear industry. The German nuclear industry seems to have developed several synthesized signal devices that monitor various plant parameters to predict and project fault conditions. These are described below.

Nuclear Detectors

No major nuclear detector programs are underway, although systems that use nuclear detector outputs to synthesize new indications are being developed.

Temperature and Pressure Sensors

Felkel (Ref. 7.7) has indicated that no new temperature or pressure sensor technologies are being developed solely for reactor applications. Fiber-optic sensors, multiplexing, and distributed processors developed for other industries are being adapted for the nuclear industry.

Other Sensor Technologies

German nuclear power plant guidelines and safety standards require monitoring and recording information on vibration, loose parts, and leakage. KWU has implemented systems to carry out these functions, as well as a fatigue monitoring system installed in the 'Convoy' plants. Table 7.2 lists the principal features of four systems. Streicher (Refs. 7.8-7.11) has described the four systems taken together as the "Series '86." The Series '86 systems are autonomous, modular systems in which event detection, alarm, data acquisition and evaluation, documentation, long-term statistics, test routines, and status checks are all performed automatically. For analyses exceeding the systems' capabilities, compressed data records are transferred to a host computer at a remote site if necessary. Operating personnel work load consists only of initial system adjustment and man-machine dialogue evaluation.

Table 7.2
German PWR Monitoring Instruments

Name	FAMOS	KÜS	SÜS	ALÜS
Monitoring	Fatigue	Loose parts	Vibration	Leakage
Sensed Parameters	Temp., Pressure, Flow	Acoustic Structure	Neutron noise, Pressure, Acceleration	Acoustic Structure
Frequency	0.25 Hz	1-10 kHz	0.1-200 kHz	100-600 kHz
Deployed	1987	1985	1987	1988

The FAMOS Fatigue Monitoring System monitors plant component temperatures, as well as primary coolant temperature, pressure, and flow. FAMOS computes stresses based on mechanical conditions and thermal history, and compares the computed stress with a precomputed three-dimensional stress calculation. System output includes crack initiation prediction, crack propagation projections, and component lifetime evaluations.

The KÜS Loose Parts Monitoring System detects and localizes loose parts by an analysis of the structure-borne burst signal which accompanies such conditions.

KÜS uses pattern recognition of time, amplitude statistics on rise time, amplitude, etc., of the burst signal in the 1-10 kHz range.

The SÜS Vibration Monitoring System detects changes in mechanical integrity such as loosening of bolts, broken springs, or vibrating pipes. SÜS monitors mechanical vibrations, pressure fluctuations, and neutron flux noise, based on coherency function and frequency spectrum analysis in the 0.0-200 kHz range.

The ALÜS Acoustic Leakage Monitoring System detects, localizes, and sizes leaks in pressurized systems. The system measures high-frequency structure- borne leakage noise in the 100-600 kHz range. The parameter of interest is the RMS amplitude of the noise as a function of time and position.

Related to the Series '86 system, Gesellschaft fur Reaktorsicherheit (GRS) mbH in Garching Germany has developed the COMOS and RAMSES system. COMOS is used in 50% of German PWRs for (quasi)-continuous monitoring and trend analysis of the signals provided by SÜS. RAMSES is a portable modem-based, computer controlled system for operator support of acoustic signature interpretation. Data are transmitted by RAMSES to a GRS laboratory for detailed analysis.

The Nuclear Research Center at Karlsruhe has developed a number of "smart" sensors and intelligent signal processing methods for reactor monitoring instruments. Many of these have been tested on the KNK II reactor there. The KNK II is a 60 Mwt sodium-cooled fast reactor; therefore, only the intelligent signal processing methods of the devices might be applicable to PWRs. Schleisiek (Ref. 7.12) has described several devices that use existing plant information but also use enhanced signal processing and analysis algorithms to synthesize new types of plant indications. Several of these synthesis instruments are summarized in Table 7.3 and described below.

Table 7.3
Karlsruhe Smart Sensors

Name	DND	LFT	KFK/IRB
Monitoring	Fuel failure size	Fuel failure location	Cooling upset
Sensed Parameters	Sodium activity Power Flow	Sodium activity Temperature Delayed neutrons	Temperature Flow Delayed neutrons

The DND and LFT instruments take signals from existing plant temperature, flow, and power instrumentation. Sodium activity and delayed neutron precursor concentration in the sodium are also measured. The DND and LFT instruments generate small amplitude control rod drive signals that produce changes in the monitored parameters. Using this information, the instruments calculate the absolute size and location of a fuel failure without operator action.

The KFK/IRB cooling upset device uses existing plant temperature and flow instruments. An algorithm computes the root mean square of the time average of the ratio of temperature and flow fluctuations. This parameter is a sensitive indicator of core cooling conditions. (There is no conventional name for this parameter, which is supposed to describe the overall state of core cooling.)

References 7.13-7.17 give several examples of the strength of combining signals to form more powerful predictors. Note especially the work of Väth et al. on detecting fuel element vibration and gas entrainment by reactivity effects and Gmeiner's report on a microprocessor-based integrated core surveillance system.

The systems described above fit into a larger class of systems being developed in Germany, the Diagnostic Expert System for Surveillance (DESYRE). DESYRE is to be an intelligent system using pattern recognition and knowledge-based approaches to formulate hypotheses about the state of the plant and to make recommendations to operators. DESYRE is to serve as an early warning indicator by combining so-called weak indicators of plant problems together to form a more powerful prediction. A DESYRE prototype is running on KNK II with 300 rules in the knowledge base and a preliminary man-machine interface.

Lastly, the Germans have developed a refinement of the traditional flux wire mapping technique in which small balls are pneumatically moved into the core and out to a detector. The system allows an operator to determine the power profile without a movable detector and associated wiring in the core.

SOVIET INSTRUMENTATION

Soviet sensor technology is based on the same phenomenologies as is U.S. technology; however, because of differences between the two countries' reactor systems, Soviet sensor technology has evolved to meet different requirements.

Nuclear Detectors

Table 7.4 lists the characteristics of one segment of a Soviet rhodium self-powered neutron detector (SPND). The VVER system uses seven of these segments as one detector in a fuel assembly, and it has 64 such monitored assemblies in a core.

The SPNDs, together with 95 in-core thermocouples, are used to measure the core power and power distribution. SPND calibration is based on a calculational model of detector performance and a large body of test statistics but no in-place comparison with movable neutron detectors.

Temperature and Pressure Sensors

No new pressure or flow sensors were presented to the panel. Nikolayenko (Ref. 7.18) described an off-line temperature-sensing technique based on measuring a change in crystal structure as a function of peak temperature. Neither the material nor the nature of the change was disclosed; however, the basic process first begins by preparing the sensitive material for a particular temperature range. The process is good to 1400°C with an accuracy of ±10°C. The material for a particular temperature range is encapsulated in rods 1 mm in diameter and 5 mm long, then installed in the object whose temperature is to be measured. Once the

Table 7.4
Soviet Detector Characteristics

Type	Self-Powered Neutron Detector
Active Element	Rhodium
Geometry	
Wire diameter (mm)	0.5 - 1.3
Casing diameter (mm)	3.0
Length (mm)	250
Insulator	MgO
Sheath	Stainless steel
Linear response upper limit (N/cm^2-s)	1×10^{17}
Response time	
Power distribution	1 minute
Protection	1 second

object has experienced its maximum temperature, the sensitive material is returned to the laboratory to be analyzed. The maximum temperature the material experienced is determined by a type of x-ray analysis. This technique is used in situations in which standard temperature measurement techniques are difficult or impossible to apply. Examples of such an application included temperature measurements of moving or rotating machinery.

Other Sensor Technologies

Yakimov (Ref. 7.19) is conducting a research and development program to measure gas concentration using semiconductors. Figure 7.3 is a schematic of a tin or zinc oxide device for measuring hydrogen concentration. The metal-oxide-resistive semiconductor sensor consists of a 0.2 mm dielectric sapphire substrate 2 x 0.5 mm with a gas-sensitive SnO_2-ZnO metal-oxide layer on one side and a platinum film 0.2 mm thick on the other side. The gas-sensitive layer may vary from 0.05 to 0.2 microns thick, depending on the device. Gold contacts 0.5 microns thick are formed on the heater and the gas-sensitive layer, and gold wire 30 microns in diameter is welded to the contacts. The sensor is mounted on a standard seven-pin base. The heater, having a resistance of 5-10 ohms, receives 0.3-0.4 watts and produces a sensor working temperature of 300-400°C. Detector sensitivity and response time are strong functions of temperature.

The conductance of the SnO_2 or ZnO layer increases with hydrogen concentration due to surface heterogeneous catalytic reactions of hydrogen reduction-oxidation with oxygen chemisorbed on the semiconductor surface. The semiconductor film is a catalyst for this reaction. The sensitivity of the detectors for hydrogen in air is 0.005-0.01 volume percent, with response time constants in the order of minutes.

These detectors are being developed for use in the nuclear industry and are to be deployed in reactor containments to measure hydrogen concentration for the purpose of controlling combustors. The sensors require that the hydrogen be carried in a dry gas stream, and this has been arranged for several systems. They have been used to measure the hydrogen concentration in the coolant of PWRs and are to be used in measuring gas concentration during fuel fabrication. Using a nickel barrier through which hydrogen can diffuse, the detectors have been used to measure hydrogen concentration in sodium.

COMPARISON WITH U.S. INSTRUMENTATION

All U.S. commercial plants operating or under construction are essentially based on designs and technologies available prior to 1977, although some backfits have been carried out. Notable among these are changes resulting from lessons

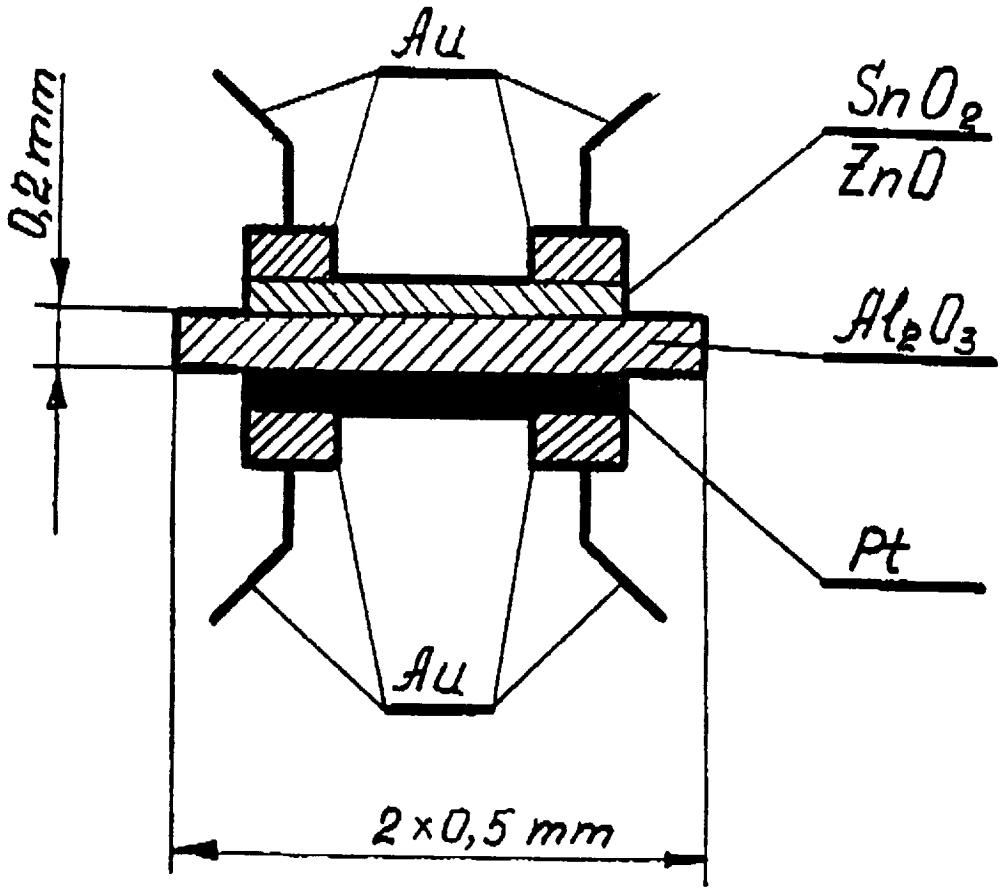


Figure 7.3. Sketch of the Oxide Sensor

learned in the Three Mile Island accident. A useful indicator of the pace of change in the U.S. nuclear industry is the observation that today, twelve years after TMI, not all plants have completed their changes. Thus, the following discussion is a comparison among snapshots taken at different technological times.

Nuclear Detectors

U.S. and European nuclear detectors all operate on the same principles, but they have been designed to meet slightly different requirements. The nominal plant in the United States would not have a nine-section in-core power detector as do the French. The decision on how many detector sections to use is based on tradeoffs specific to each country and not on technological breakthroughs.

Nevertheless, the French program to develop one neutron detector to cover all power ranges does offer the significant advantage of reducing the number of detectors, cabling, and penetrations, thus producing significant economic saving. Similarly, the French development of in-core fission chambers with dimensions similar to SPNDs would eliminate the need for the in-core calibration guide tubes, vessel penetrations, and movable detectors presently in use.

The Soviet decision to use a statistical algorithm rather than movable fission chambers to calibrate SPNDs is interesting, especially since MgO is used as the insulator. MgO is known to deteriorate under irradiation, as compared with Al_2O_3. The calibration algorithm must not only correct for unavoidable changes in emitter burnup and self-absorption, but also for insulator resistance changes. This complicates the correction calculation and must increase the uncertainty associated with the calibration. Ultimately, the required accuracy of the calibration depends in part on the thermal hydraulic design margins used in the core design, and these are different for Soviet versus U.S. reactors.

No new German nuclear detectors were reviewed.

Temperature and Pressure Sensors

The Soviet off-line crystalline temperature detector is not applicable to plant monitoring and control, although it may have application to long-term monitoring akin to in-vessel metallographic specimens.

No new French or German temperature/pressure sensor technologies were reviewed.

Other Sensor Technologies

The French synthesis instruments for core temperature and axial power offset control by rod position are a developed technology but not a conceptual leap in instrumentation. (These systems are also discussed in Chapter 5.) The French have also developed combined diagnostic instruments as described in Papin (Ref. 7.20).

The German Series '86 instruments are systems which are similar to U.S. systems in terms of primary sensor input, although the autonomy of the German systems seems to be much greater than that of U.S. equipment. The KFK/IRB cooling upset instrument seems to be akin to a noise analysis approach to monitoring plant conditions, in that it produces a signal that is not a convolution of traditional parameters, e.g., power-to-flow ratio. Exactly what this instrument tells the operator or what action the operator should take based on its signal is not clear to the panel. It seems to be a precursor indication of deteriorating core conditions and thus may be useful in the future because sensitive indications of core conditions are always being sought.

Fiber-optic sensors are an important part of the French instrument development program. U.S. utilities, both directly and indirectly via the Electric Power Research Institute (Ref. 7.21), support a fiber-optic sensor development program. Point and distributed temperature and pressure sensors have been developed in the United States and are available commercially. Programs using fiber optics are underway to measure strain, process water chemistry, and almost every parameter important to plant operation.

Post-Accident Instrument Development

The Three Mile Island, Unit 2, accident is the most severe reactor accident that has occurred in the United States, and the Chernobyl accident occupies the same place in the U.S.S.R. Both these countries have developed reactor instrumentation specifically for such severe accidents. Major references for this topic are the Nuclear Regulatory Commission publications, *NRC Action Plan Developed as a Result of the TMI-2 Accident* (Ref. 7.22) and *Implications of the Accident at Chernobyl for Safety Regulation of Commercial Nuclear Power Plants in the United States* (Ref. 7.23).

Significant instrument development programs were begun in the United States following the TMI accident. Instruments for measuring exhaust gas stack activity, containment activity, and area radiation were hardened, and their measurement ranges were increased. A safety parameter display panel was developed to show important plant conditions. A reactor vessel water level monitoring device was

mandated for PWRs. This device required a significant development effort, as each of the vendors sought to satisfy the NRC requirement.

In *Implications of the Accident at Chernobyl*, the NRC concluded that no additional instrumentation needed to be developed in the United States as a result of the Chernobyl accident. The U.S.S.R. has, of course, enhanced its radiation monitoring and power level measurement instruments as a result of Chernobyl.

The panel saw no new devices in Europe that were developed specifically in response to the TMI or Chernobyl accidents.

SUMMARY

Table 7.5 summarizes the major findings of the instrumentation review. A "+" in a position in the table indicates some development that may offer improvements in simplicity, reliability, and/or cost over U.S. instrumentation. The panel found no evidence of fundamental instrumentation differences between Europe and the United States.

Table 7.5
Comparison of European with U.S. Instrumentation Technology

	France	Germany	USSR
Pressure	-	-	-
Temperature	-	-	-
Neutron flux	+	-	+
Flow	-	-	-
Level	-	-	-
Gas	-	-	-
Vibration	-	+	-
Gamma	-	-	-

+ Indicates a comparative advantage over U.S. technology

Instrumentation technologies are evolutionary. Although several European technologies seen by the panel offer enhancements over U.S. technology, no enabling technologies were apparent; however, several devices seem to warrant further investigation. These include (1) the French enhanced power range neutron detector, (2) German plant performance indicator synthesis, and (3) Soviet SPND calibration by calculation.

REFERENCES

1. Furet, J. Chef De Service, Instrumentation et Systems Nucléaires, Centre D'Études Nucléaires De Saclay, F 91191 Gif-Sur-Yvette, Cedex, France. Personal communication, November, 1990.

2. Parry, A. Manager, Instrumentation and Control Department, Framatome, Tour Fiat, Cedex 16, 92084 Paris LaDefense, France. Personal communication, November, 1990.

3. Breuzè, G. and J. Serre. "Fiber Optic Components Compatibility with the PWR Containment Radiation Field," IAEA Specialists' Meeting on Communication And Data Transfer in Nuclear Power Plants, Lyon, France, 24-26 April 1990.

4. Tallec, M., Staff, Division d'Électronique, de Technologie et d'Instrumentation, Centre D'Études Nucléaires De Saclay, F 91191 Gif-Sur-Yvette, Cedex, France, Personal Communication, November 1990.

5. Leroy, J. L., J. P. Millot, and M. Troublè. "Control Rod Cluster Assembly Command Method For Load Following PWRs Without Using Boration Changes," International Conference on the Physics of Reactors: Operation, Design and Computation, Marseille, France, 23-27 April 1990.

6. Felkel, L. Dipl.-Inform., Information Concepts Subsection, Systems Division, Gessellschaft für Reaktorsicherheit (GRS) mbH, Reactor Safety Company Ltd., Forschungsgelaende, D-8046 Garching, Germany. Personal communication.

7. Felkel, L. See Ref. 7.6.

8. Streicher, V., P. Jax, and H. J. Wehling. "Recently Developed KWU Systems For Monitoring Fatigue, Vibrations, Leakages and Loose Parts In Reactor Circuits." IAEA CN-49/91. Proceedings of Man-Machine Interface in the Nuclear Industry Conference, Tokyo, 15-19 February 1988.

9. Siemen AG, Bereich Energieerzeugun, (KWU) E22, Mebtechnik, DV-und Überwachungssysteme, D-8520, Erlangen, Germany. "Ultra-Sonic Liquid Level Monitoring," Power Generation Group. Company Brochure, 1990.

10. Siemen AG, Bereich Energieerzeugun, (KWU) E22, Mebtechnik, DV-und Überwachungssysteme, D-8520, Erlangen, Germany. "Vibration Monitoring System," KWU Group, Company Brochure, 1990.

11. Siemens AG, Bereich Energieerzeugun, (KWU) E22, Mebtechnik, DV-und Überwachungsstystem, D-8520, Erlangen, Germany. "Acoustic Leakage Monitoring System," Power Generation Group, Company Brochure, 1990.

12. Schleisiek, K. "Development of 'Smart' Sensors and Intelligent Signal Processing Methods." KFK Institute for Reactor Development. Personal communication, 1990.

13. Väth, W., F. Mitzel, and S. Ansari. "Identification of Vibrational Effects in KNK II Fuel Elements." Institut fur Neutronenphysik und Reaktortechnik Projekt Schneller Bruter, Internal Report, Karlsruhe, Germany, July 1981.

14. Gmeiner, L. "Microprocessor-Based Integrated LMFBR Core Surveillance." Institut fur Datenverarbeitung in der Technik Projekt Schneller Bruter, Internal Report, Karlsruhe, Germany, June 1984.

15. Hoppe, P., H. Massier, F. Mitzel, and W. Vath. "Untersuchungen zum Gaseintrag an KNK II." Institut fur Neutronenphysik und Reaktortechnik Projekt Schneller Bruter, Internal Report, Karlsruhe, Germany, November 1979.

16. Mitzel, F., W. Väth, and S. Ansari. "Nachweis von Brennelement-schwingungen in KNK II." Institut fur Neutronenphysik und Reaktortechnik Projekt Schneller Bruter, Internal Report, Karlsruhe, Germany, November 1982.

17. Väth, W., F. Mitzel, and S. Ansari. "Identification of Vibrational Effects in KNK II Fuel Elements." Institut fur Neutronenphysik und Reaktortechnik Projekt Schneller Bruter, Internal report, Karlsruhe, Germany, July 1981.

18. Nikolayenko, V. A. Kurchatov Institute of Atomic Energy, Kurchatov Sq., 123182, Moscow, U.S.S.R. Personal communication, December 1990.

19. Yakimov, S. S. "Sensor Diagnostics of Hydrogen In Nuclear Power." Kurchatov Institute of Atomic Energy, Moscow, USSR, Internal Report, December 1990.

20. Papin, B., and J.L. Voitellier. "Advanced Operator's Aids and Control for French FBRs, Present and Future," paper presented at IAEA International Working Group for Fast Reactors Meeting, Argonne, Illinois, 1989.

21. Electric Power Research Institute. *Proceedings of Fiber Optics Workshop.* EPRI Report ER-6537, 1989.

22. U.S. Nuclear Regulatory Commission. "NRC Action Plan Developed as a Result of the TMI-2 Accident" Vol. 1, NUREG-0660, May 1980.

23. U.S. Nuclear Regulatory Commission. "Implications of the Accident at Chernobyl for Safety Regulation of Commercial Nuclear Power Plants in the United States" Vol. 1, NUREG-1251.

CHAPTER 8

COMPUTER STANDARDS AND TOOLS

Leo Beltracchi

INTRODUCTION

This chapter presents the panel's assessment of computer standards and tools used in the control and information systems of the European nuclear industry. The survey covered the primary topics of software engineering, databases, and user interface management systems, and the following subtopics:

SOFTWARE ENGINEERING
- Standards
- Tools
- Design and Test Research
- Engineering Simulators

DATABASES

USER INTERFACE MANAGEMENT SYSTEMS
- Graphic Languages
- Design Tools
- Design Techniques

Assessment Process

The assessment process included a literature review of European work in the subject areas, a visit to the leading research groups and institutions in Europe, and an analysis of technical papers and information provided by the panel's European hosts. The literature survey identified standards and technical papers on software

engineering design, test techniques, and tools, as well as technical papers describing human-process interface models and design methods. After reviewing this material, the panel prepared a survey instrument (Appendix 8.A) as an aid in conducting technical interviews.

In its survey of computer standards and tools, the panel visited organizations in France, Germany, and the Soviet Union from 26 November to 5 December 1990. The French organizations surveyed were Framatome, Électricité de France (EDF), the Centre d'Études Nucléaires de Saclay, and the CEA Institut de Protection et de Sûreté Nucléaire. The German organizations surveyed were Siemens AG, Gesellschaft für Reaktorsicherheit (GRS) mbH, and the ISAR 2 nuclear power plant. The Soviet organizations surveyed were the Kurchatov Institute and the Institute of Control Problems. All of these organizations were very gracious hosts and provided access to their experts in support of the survey. Technical discussions with these experts were extensive, deep, and open.

Survey Objectives

The panel investigated the topic areas of this chapter in light of the following four objectives:

1. Evaluate and describe the state of the art of computer standards and tools in the European nuclear industry

2. Compare the European state of the art with that in the United States

3. Extrapolate from the current state of the art to future states

4. Evaluate the impact and implications of European research and accomplishments

The following is a brief review of computer standards in the U.S. nuclear industry to help place in context the discussion of survey results.

Evolution of Computer Standards in the U.S. Nuclear Industry

The U.S. nuclear industry has a rich history in the development and use of design standards. A 1972 example of a design standard for nuclear power plant safety systems is IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Station" (Ref. 8.1). This standard documents the minimum requirements for the safety-related functional performance and reliability of protection systems for nuclear power plants. Although this standard does not forbid the use of digital computers for safety systems, the requirements in this standard reflect design and operational experience with analog hard-wired technology.

The use of digital computers in the monitoring of nuclear power plant performance has led to the development and publication of design and development guidelines. In the late 1960s, Gimmy identified guidelines for computer-based monitoring of reactor performance at the Savannah River Plant, a production facility where three large reactors are each equipped with an on-line digital computer that has over 3000 analog inputs and serves control room operators 24 hours a day (Ref. 8.2). Gimmy states that the reliability of the computer-based system must be high for operators to accept the technology. The following three guidelines, still useful today, are discussed in detail:

1. Computer output should be simple and in a form needed by operators

2. Resources should be allocated for computer repair, and computer programs should allow for minor sensor faults

3. A quality assurance system of cross-checks and auditing should be an integral part of the programming

In a 1977 work, Gimmy describes the design and operational use of digital computers in the protection system for the Savannah River Reactors (Ref. 8.3). The paper deals with the approach to two problem areas that confront any computerized protection system:

1. How to ensure signal accuracy and proper response to real changes but reject the spurious signals that are bound to occur

2. How to develop and test computer software so that it will be as reliable as hard-wired logic circuits

In this paper Gimmy discusses and identifies guidelines for the validation of signals from differential pressure transducers. These transducers are useful in measuring coolant flow. Gimmy also provides guidelines for the development and testing of computer-based protection systems. After normal debugging and integration into an operating system, a failure-response test was made. This detailed test used deliberately induced failures in the computer and data inputs to force the software down seldom-used branches of the logic. Today, this type of testing, so-called structural testing, is an accepted practice in the evaluation of software.

In a 1984 work, Gimmy describes an expert system to aid operators in responding to multiple alarms in a developing incident (Ref. 8.4). The system, called "Diagnosis of Multiple Alarms," uses existing control computers to analyze the pattern of alarms that accompany a leak from the primary or secondary coolant system. The computer provides a message on a video display unit to indicate the type and location of the leak. This is one of the first uses of an expert system to

aid reactor operators in decision-making tasks. The paper presents and discusses several useful guidelines on the design and evaluation of expert systems.

Combustion Engineering has designed and developed a digital-computer-based protection system for a commercial nuclear power plant (Ref. 8.5). This is the Core Protection Calculator System (CPCS) now operational at Arkansas Nuclear One, Unit-2. This system initiates a reactor trip whenever the departure-from-nucleate-boiling ratio (DNBR) or the linear power density (LPD) exceeds limiting values. Six programmable digital computers read and process sensor data to accomplish the protection function. The remainder of the protection system consists of conventional hard-wired equipment.

References 8.6-8.9 describe the safety evaluation of the CPCS by the U.S. Nuclear Regulatory Commission (USNRC). The safety evaluation resulted in many design, development, and test issues, all of which were resolved prior to system licensing in late 1978. Reference 8.5 discusses some of the problems in the validation of safety system software. Reference 8.10 discusses the reliability, qualification, and documentation of safety system software. Reference 8.11, the American National Standards Institute's ANSI/IEEE-ANS-7-4.3.2-1982, describes a standard that embodies many of the lessons learned in the design, development, testing, and safety evaluation of the CPCS. This standard establishes a means for promoting safe practices for the design and evaluation of safety system performance and reliability. The standard places a heavy emphasis on the design verification and validation of software in achieving reliable software. USNRC endorsed this standard through a regulatory guide (Ref. 8.12).

SOFTWARE ENGINEERING

The software engineering subjects the panel surveyed consisted of standards, tools, design and test research, and engineering simulators.

Standards for Software Designs

The main focus of the standards survey was on computer-based safety systems for nuclear power plants. Nuclear power plant safety systems must be highly reliable in the performance of their function. To minimize errors in the product, the process of designing a safety system must be structured and thorough.

Standards and guidelines for the design of safety systems were found during the survey. Reference 8.13 is a book that resulted from the European Workshop on Industrial Computer Systems, Technical Committee 7 (EWICS TC7). This book presents guidelines for the design, development, and acceptance of critical computer systems. The failure of critical computer systems may affect the health

and safety of the public. These guidelines address many subjects, such as software quality assurance measures and the maintenance and modification of safety-related computer systems. Further, each subject has a checklist. The checklist is useful to a designer and to a verifier in evaluating conformance to the guidelines. The integration of the guidelines and a checklist for many subjects makes this book a useful design document. During the survey, the panel found that all organizations designing computer-based safety systems were using these guidelines and checklists.

IEC Standard 880, "Software for Computers in the Safety Systems of Nuclear Power Stations," was published in 1986 (Ref. 8.14). The elements of this standard address many phases of the software life cycle, consisting of requirements analysis, design, coding, verification, hardware/software integration, validation, and maintenance. The standard's appendices provide details on such matters as system development life cycle, software performance specifications, and software testing. This standard covers the major phases of the software life cycle. Organizations surveyed in France, Germany, and the U.S.S.R. stated they were conforming to IEC Standard 880 in developing computer-based safety systems. Reference 8.15 describes the development and qualification of a digital-based protection system in France.

EDF operates 54 nuclear units, 500 hydroelectric plants and 140 energy control centers, and communication networks will play a key role in the rapid development of its computer-based control and supervisory systems.

SPRINT specifications consist in a selection of a number of OSI Protocols together with additions necessary to achieve interoperability in a multi-vendor environment. They provide a common basis for specifying the communication networks and defining requirements for vendors.

Based on the OPEN SYSTEMS INTERCONNECTIONS (OSI) 7 layer stack of protocols, the SPRINT specifications are divided in two parts:

> SPRINT 14 deals with the OSI first four layers and describes how to offer the OSI connection mode Transport Service on different possible subnetworks, and defines relaying strategies between subnetworks as well as addressing structure;
>
> SPRINT 57 describes layers 5 to 7 stacks that offer application layer services such as file or message transfer.

The first SPRINT network is a local area network installed at the CRUAS nuclear power plant. It allows each new computer to access a common database while being provided with common facilities like application configuration services and

gateways to other networks (local or long distance). Similar networks will be installed in all the nuclear sites by 1992.

The second SPRINT application is scheduled to begin in late 1992 and is the nationwide backbone of the energy management system (built on top of a private X 25 subnetwork).

The British Interim Defense Standard 00-55, "Requirements for the Procurement of Safety Critical Software in Defence Equipment," was issued in the United Kingdom in May of 1988 (Ref. 8.16). This comprehensive standard contains elements on safety management, software engineering practices, and the project life cycle. Within software engineering practices, it addresses hazard analysis, safety integrity analysis, specification, design reviews, unacceptable practices, and others. This standard requires the use of formal specification and design techniques. It considers conventional design methods inadequate for the development of high-integrity software. Further, the standard identifies several software engineering practices as unacceptable, e.g., the liberal use of "GO TO" instructions and interrupts. Although the Interim Defense Standard is a military standard, it has received considerable attention in the European and U.S. nuclear industries. This attention has focused on formal specification and design techniques and the unacceptable practices. While many organizations in the survey were aware of the standard, no one had adopted the standard for use in the nuclear industry. However, there is research under way on the use of formal methods; this is discussed in the Software Design and Test Research section later in the chapter.

The nuclear industry in the United States does not now have a standard that is equivalent to IEC Standard 880 or the guidelines in Critical Computer Systems 2 (Ref. 8.13). However, there is an effort in progress to develop an equivalent standard. This effort is the revision to ANSI/IEEE/ANS 7-4.3.2-1982, "Application Criteria for Programmable Digital Computer Systems in Nuclear Power Generating Stations." This standard development effort involves individuals from nuclear utilities, vendors, and the USNRC.

Summary of European Software Design Standards

ANALYSIS

1. Standards and guidelines are the basis of the design and development of computer-based safety systems.

COMPARISON

1. The U.S. nuclear industry does not now have equivalent standards and guidelines for the development of computer-based safety systems; however, an effort to develop equivalent standards is under way.

EXTRAPOLATION

1. Operational experience in the use of computer-based safety systems is necessary to refinement and upgrading of standards and guidelines.

Computer-Aided Software Engineering (CASE) Tools

Computer-aided software engineering tools aid designers in development of computer programs. A CASE tool supports one or more phases of the life cycle. CASE tools aid designers in analysis tasks, design, coding, testing, implementation, and maintenance (Ref. 8.17). The use of CASE tools adds discipline to the development process, thereby reducing the potential for human error.

Several CASE tools were found during the survey. One of the first tools was the Specification Application Generation Automatic (SAGA) software (Ref. 8.18). The authors describe this tool as a software design workshop that aids in the life cycle phases from specification through coding. The features of this tool are (1) a synchronous data flow specification language, (2) an interactive graphic support of this language, (3) a top-down design by successive refinements, (4) consistency and complexity limitation checks, and (5) the ability to reuse certified components.

The SAGA workshop serves as a tool for development of digital-computer-driven displays and controls for France's 1500 MWe N4 nuclear power plants. Experience in the use of SAGA has resulted in significantly shorter design and coding phases, in addition to a common language for communication within the project (Ref. 8.18).

The SAGA workshop is also serving in the development of a digital protection system. This tool aided in the analysis and graphic specification of the computer program. Encoding occurs directly from preliminary and detailed designs specifications by translating them (via SAGA) into code (Ref. 8.19).

Another CASE tool seen during the survey of France was OST (Ref. 8.20). OST allows a user to describe realtime multimicroprocessor systems, perform dynamic simulations, and store results for later analysis. The simulation works instruction by instruction, and with the use of OST, the human user can modify and control this environment. This allows for intensive study and testing of the code in detecting and correcting faults. In the simulation of a system, the exact

microprocessor code is not necessary. The objective of OST is to simulate, on a host computer, the behavior of realtime software implemented on one or more microprocessors. It has the capability to describe its environment and to modify it easily for the validation of the software. OST is capable of simulating the following microprocessors: M6800, INT8086, M68000, and M6809.

Nuclear safety authorities in France are using OST in their studies of microprocessor-based safety systems. OST is a powerful design tool in the requirements and specification phase of the development process. These phases are critical ones because of the difficulty of verifying the relationships among the various requirements and the completeness of each phase. The detection and correction of errors in these early phases of the development cycle enhance integrity and minimize cost of the final software. OST is also useful in the dynamic analysis of realtime software. Figure 8.1 illustrates how the nuclear safety authorities use OST in the back-to-back testing of safety-related software.

Figure 8.2 is an example of the software life cycle used by the nuclear safety authorities in France. There are seven phases to the life cycle: (1) the requirements specification phase, (2) the functional specification phase, (3) the architectural design phase, (4) the detailed design phase, (5) the coding and implementation phase, (6) the integration testing and commissioning phase, and (7) the operation, maintenance, and enhancement phase. This life cycle is very similar to the life cycle used in the United States.

A microprocessor-based protection system is under development at Siemens AG KWU in Germany, where an in-house-generated CASE tool named Specification and Coding Environment (SPACE) is being used (Ref. 8.21). This tool has a semantically direct specification language and uses graphical symbols for syntax. The use of graphical syntax aids in its translation into code. SPACE was developed in-house to meet specific requirements not available in commercially available CASE tools.

SOSAT is a CASE tool principally developed at the OECD Halden Reactor Project (Ref. 8.22). This tool can analyze programs implemented on a variety of microprocessors. A disassembler extracts the program from a hexadecimal memory dump of the processor and translates it into common assembly language CAL. The CAL code forms the basis for further analysis. The development of this CASE tool was a joint project of the OECD Halden Project, Technische Uberwachungsverein Norddeutschland, and Gesellschaft für Reaktorsicherheit.
SOSAT is a tool that automates many tasks in the analysis and testing of programs stored on a variety of microprocessors. The following functions are available from SOSAT:

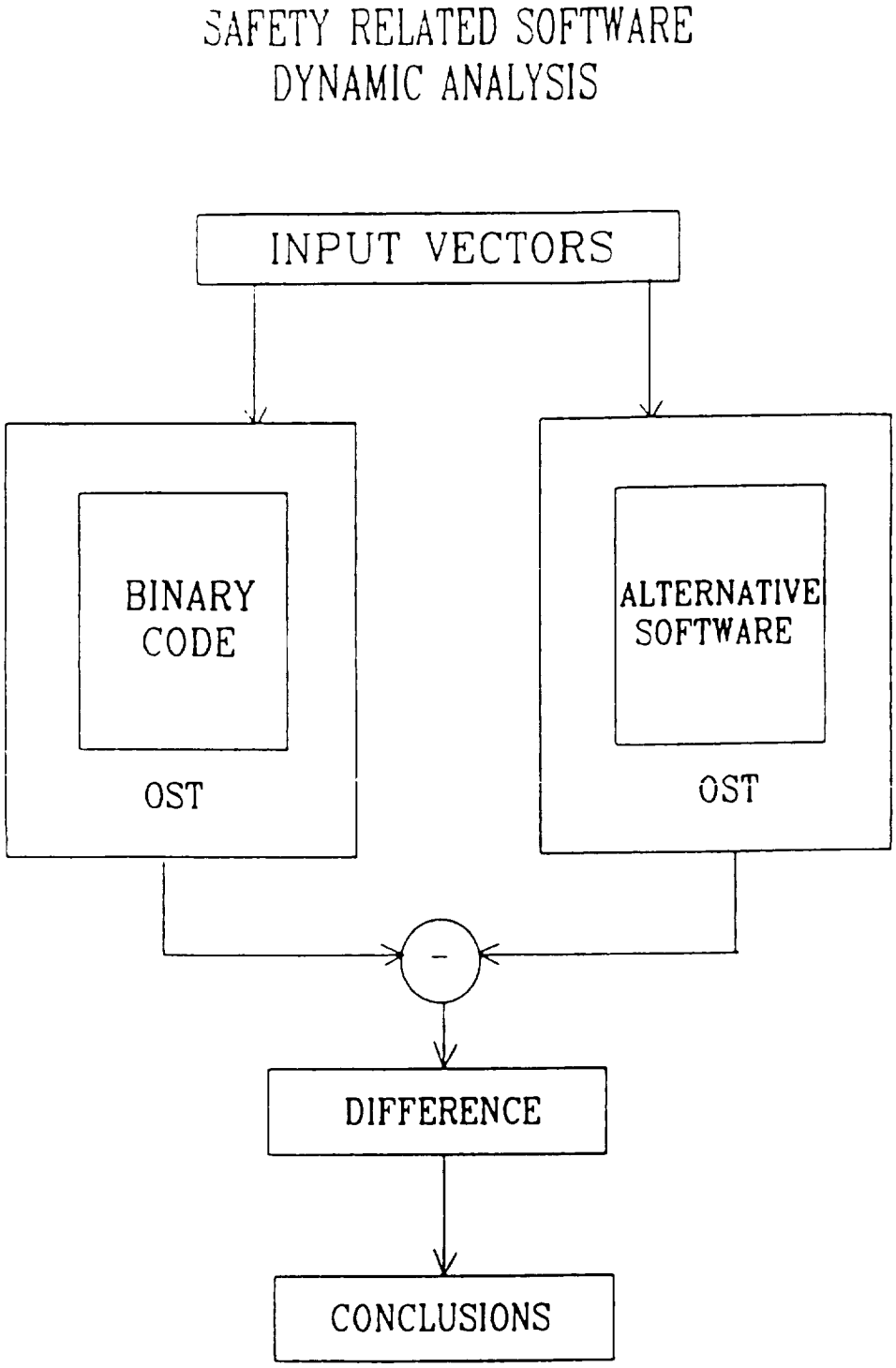


Figure 8.1. OST and Software Dynamic Analysis

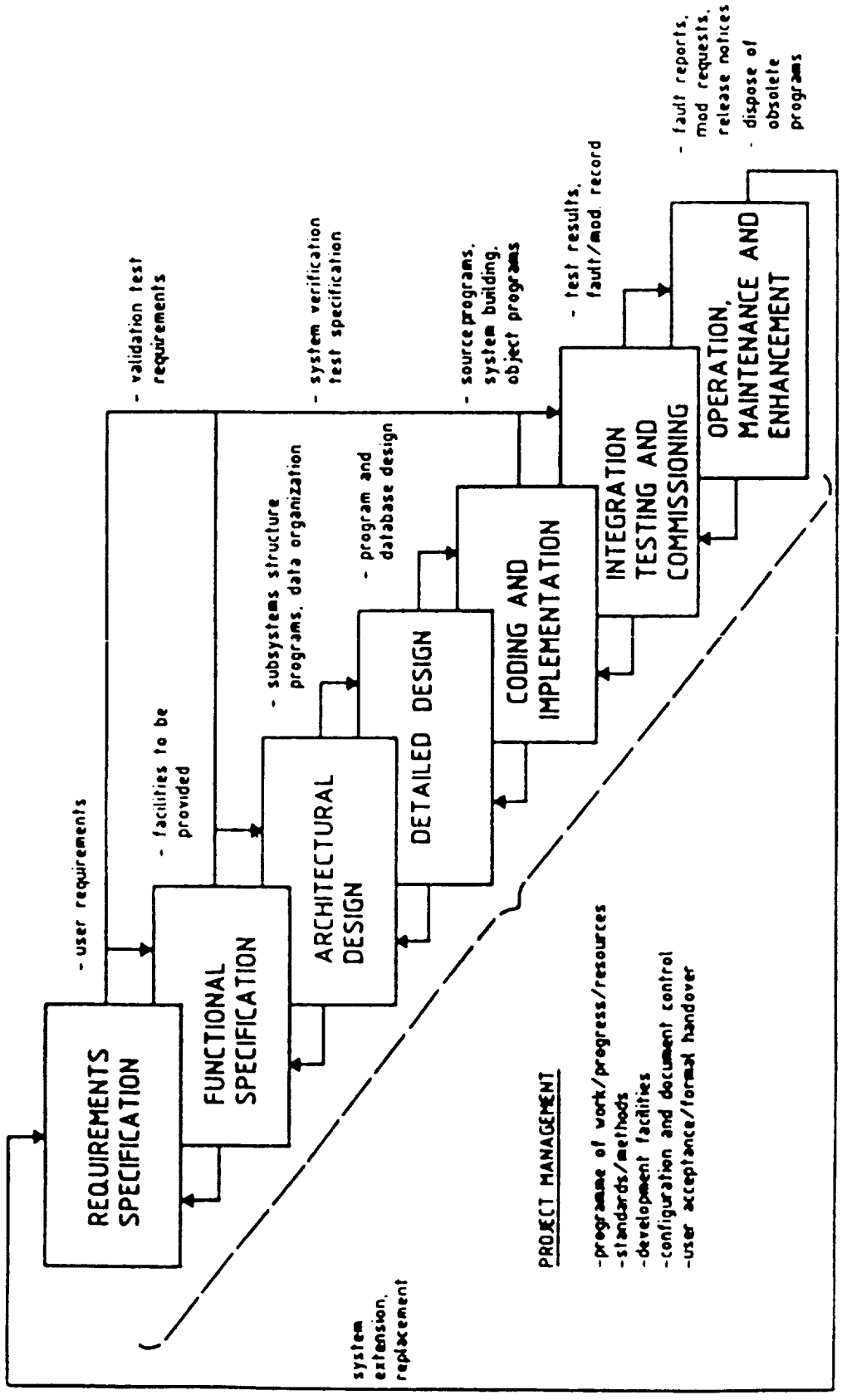


Figure 8.2. Software Life Cycle Observed by French Nuclear Safety Authorities

1. Metric computations. SOSAT performs software measures consisting of a count of the number of bytes, number of jumps, branches, I/O instructions, interrupts, etc., in the source program. It also evaluates measures based on Halstead Software Science: volume, length, effort, etc. (Ref. 8.23).

2. Static Analysis. In the structural analysis, SOSAT converts the code into directed graphs. If division into graphs is not possible, it implies a serious structural weakness and possible source of error. In the path analysis, SOSAT aids in the generation of test data to ensure that the analyzed code can be tested by a minimum number of test runs.

3. Dynamic Analysis. In dynamic analysis, SOSAT instruments the program with counters and screen input/output so that a user can follow the execution of the program with selected data. This aids in the debugging and the testing of the code.

An effort is under way to enhance SOSAT with the addition of analysis modules to facilitate the comparison of the final program with the original specification. If successful, this will serve an important function in the verification of the code to the specifications. The SOSAT tools are best suited to analyze program modules of limited size, e.g., digital replacement of logic circuits in safety critical systems. The tool can handle larger programs, but interpretation of results is very laborious. Finally, licensing authorities (Technische Uberwachungsverein Norddeutschland) are now using SOSAT in the assessment of a microprocessor-based safety system (Ref. 8.22).

Evidence of CASE tool development and use also exists in the Soviet Union. Reference 8.24 contains a short discussion on the development of an expert system for generating Fortran codes. The codes developed with the expert system are for three-dimensional neutron-physics reactor calculations.

Tool Assessment and the Waterfall Model

The waterfall model of the software life cycle provides an overview of the design and development process (Ref. 8.25). The reference also discusses the spiral model of software development; however, the following discussion of the development process is limited to the waterfall model.

The design and development of software for critical applications such as safety systems is a complex, detail-intensive process. The waterfall model identifies a means of dividing the process into functional phases to facilitate management and control of the process. Figure 8.3 identifies the phases in the model.

The first phase assesses the feasibility of the software project. The second phase performs a requirements analysis to identify functions. The design and detailed design phases decompose the functions into tasks and subtasks. The results from the analysis of tasks and subtasks are the basis for specifications for the code. The next phase is the coding of the specifications and the test of units of code. In the sixth phase, units are integrated into subprograms and with the final hardware and then tested. In the system test phase, the integrated program is validated against the functions in the requirements phase. In the eighth phase, the validated system is installed and checked for operation. Maintenance is performed on the software to improve its functional performance and to correct errors undetected during its design. In the final phase, the software is retired because it is difficult to maintain or because a better product exists.

Figure 8.4 identifies where in the life cycle phases the previously discussed CASE tools fit: SAGA and SPACE are helpful in the requirements phase; OST, SAGA, and SPACE are useful in the design, detailed design, and code and unit test phases of the life cycle; finally, OST and SOSAT are useful in the system test phase. No one CASE tool is useful over the total life cycle. From the information available, it was difficult to evaluate the scope and depth of coverage of a CASE tool for a specific phase. What is clear, however, is that the European nuclear industry is making ample use of CASE tools over many phases of the life cycle.

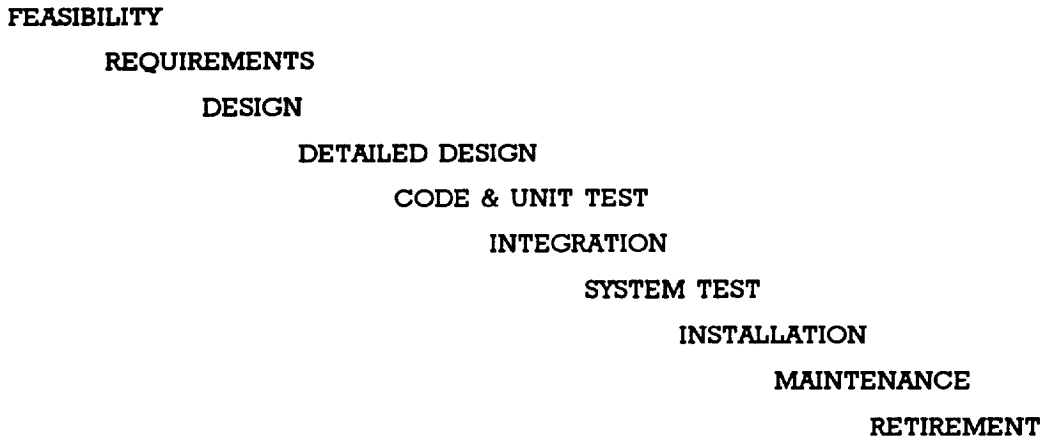


Figure 8.3. Typical Phases of the Waterfall Model of the Software Life Cycle

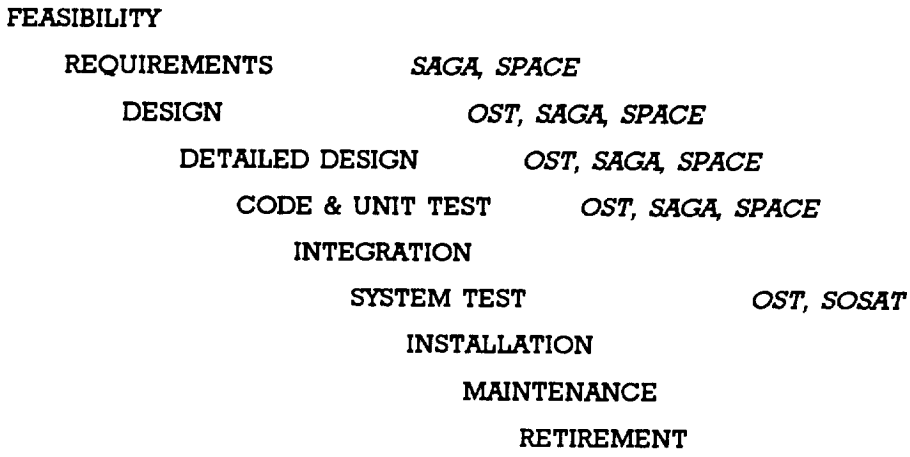


Figure 8.4. Placement of European CASE Tools in the Waterfall Model

Summary of European Use of CASE Tools

ANALYSIS

1. Tools used in the life cycle reduce the potential for errors in the final software because of the discipline provided by the use of the tools.

2. The use of CASE tools generate data, e.g., structural test coverage, useful in the final engineering judgment on the acceptance or rejection of the program.

3. It was difficult to determine the amount and quality of aid provided by a CASE tool for a specific phase of the software life cycle.

COMPARISON

1. It is the author's opinion that the U.S. Nuclear Industry's use of CASE tools is minimal in comparison to European use of tools.

EXTRAPOLATION

1. In due time, the European nuclear industry will use a comprehensive CASE tool set for all phases of the life cycle in software development.

Software Design And Test Research

Research on the design and test of high-integrity software is underway within the nuclear industry in Europe. The text that follows discusses each of these activities.

In discussions at GRS Garching (Ref. 8.26), the panel learned of an ESPRIT Project named DARTS, Demonstration of Advanced Reliability Techniques for safety-related computer systems. This ESPRIT Project will use different methods and teams to generate and test safety system software. Four teams from various European countries are participating in the project. Two teams are to use diverse formal methods in the design and development of the code; two teams are to use diverse conventional methods in the design and development of the code. Once the codes are developed, back-to-back testing methods will evaluate the codes. The project will collect design and test data for each development method used. The main goal of this project is the evaluation of different design and development techniques in terms of effort required and reliability achieved; this includes the assessment of fault-tolerant architectures consisting of more diverse versions. This is a four-year project which started in 1989. The highly qualified researcher in charge of the project has authored several technical papers on the subject (Refs. 8.27-8.30).

Research is also under way on the design and test of safety system software at the OECD Halden Reactor Project (Refs. 8.22, 8.31, and 8.32). Reference 8.31 reports research results for the design and test of diversely produced programs for the goal of enhancing safety. The research was a multinational effort. The Safety and Reliability Directorate in the United Kingdom developed a specification for a safety system, and three independent teams coded the specification: (1) a team at the Halden Reactor Project, (2) a team at the Technical Research Center of Finland, and (3) a team at the Central Electricity Research Center in the United Kingdom. Although the research investigated many issues, the discussion that follows focuses only on the fault-finding strategies and test data selection investigated.

The Halden Reactor Project used several different test data types consisting of deterministic data and random data. The deterministic data consisted of:

1. Systematic data manually produced to test the functions identified in the specification of the software

2. Acceptance test data and corresponding expected results based on a team's understanding of the problem

The random data consisted of:

1. Uniform distribution of test cases within the high and low range of the input data

2. Gaussian distribution of test cases with the mean in the mid-range of the input data

3. Uniform distribution of test cases at the boundaries of the input data

4. Gaussian distribution of test cases at the boundaries of the input data

In evaluating test data efficiency, each program developed in the project was seeded with 62 faults, then each program was tested back-to-back with the same input data type. The researchers found all seeded faults, but multiple data types were necessary to do so. The most efficient data types in detecting seeded faults were the uniform distribution of test cases within the high and low range of the input data and the Gaussian distribution of test cases at the boundaries of the input data. The least efficient data types were the Gaussian distribution of test cases with the mean in the mid-range of the input data and systematic data. Table 8.1 contains the results from this study.

These results are extremely interesting. The use of systematic test data is necessary to show that the software meets the functions stated in the design specification. However, while the use of systematic data is necessary, it is not sufficient. The use of other test data such as a uniform distribution of test cases within the input data range in conjunction with a Gaussian distribution of test cases at the boundaries of the input data is also necessary. The use of these test cases may flush out unintended functions in the code. This certainly was the case for the seeded errors. From the results in Table 8.1, it would appear that testing with both systematic data and random data are necessary.

The research results on test strategy represent only one experiment; however, other related data exist. During the late 1970s, the Core Protection Calculator System (CPCS) discussed earlier in this chapter was reviewed and ultimately licensed by the U.S. Nuclear Regulatory Commission (Refs. 8.6-8.8). This system is a digital-computer-based protection system for a nuclear power plant. The test strategy used in this effort was very similar to the combination of uniform distribution of test cases within the input data range and the Gaussian distribution of test cases at the boundaries. The CPCS has operated successfully for over a decade.

Table 8.1

Fault Detection Performance With Different Test Data Using 62 Seeded Faults

TEST DATA	1000 TEST CYCLES		ALL TEST CYCLES*	
	Detected	Undetected	Detected	Undetected
Acceptance Data	55	7	55	7
Systematic Data	49	13	50	12
Uniform Random	56	6	61	1
Gaussian Random	42	20	49	13
Uniform Boundary	49	13	56	6
Gaussian Boundary	51	11	57	5

More than 600,000 data sets

The survey asked all participants about the type of test strategy used in their software test programs. No one was using a test strategy that contained random data.

Summary of European Software Design and Test Research

ANALYSIS

1. An active research effort exists within Europe to evaluate the use of formal methods in the design and development of safety systems.

2. The use of random data as part of a test strategy appears to be useful, but it does not exist in practice.

COMPARISON

1. U.S. research exists on software for high-integrity systems such as safety systems, but this research is outside of the nuclear industry.

2. Some use of random data as a test strategy exists in the U.S. nuclear industry, but it is rare.

EXTRAPOLATION

1. Research and progress on design and testing of software will be slow and costly.

Engineering Simulators

Two workstation-based engineering simulators useful in the design of nuclear power plants were found during the survey in France (Refs. 8.33-8.35). OASIS (Ref. 8.33) is a workstation-based simulator (under development) initially developed for France's fast breeder reactor program. Its planned uses are in safety and design studies for normal, disturbance, and accident conditions. In its current form, OASIS is being used in the study of problems involving decay heat removal through the emergency circuits of SUPER PHENIX 1.

OASIS consists of many parts, the main part of which is the interactive database, PROBASE. This database contains all dynamic variables for the reactor at any instant of time. Another part of OASIS is MISCENE; it is the equivalent of a simulation code and calculates the state of the reactor at each instant of time. Presently, by using the modular PWR simulation code CORIANDRE instead of MISCENE, OASIS can be used for the representation of any kind of PWR as well as for FBRs. The man-machine interface, a control panel, is the function of SYVIC. Still another part is DANAOSS (under development, Ref. 8.34), an artificial-intelligence-based module to provide on-line analysis of transients.

SIPA-2 (Ref. 8.35) is a workstation-based simulator used by the personnel at CEA Institut de Protection et de Sûreté Nucléaire to study pressurized water reactors. The specific uses of the workstation are for safety analyses, safety drills, and training engineers. SIPA-2 models the primary coolant circuit and part of the secondary coolant circuit; related systems such as primary process controls; secondary process controls; the protection system; the safeguard system, and containment. SIPA-2 is based on the advanced code CATHARE-SIMU, a version of the advanced thermal-hydraulic computer code CATHARE developed by EDF and CEA. As a first step, SIPA-2 will have the description and the data of the PWR series CP1 (900 MWe, 3 loops) and P4 (1300 MWe, 4 loops) reactors. Most of the plant models will be developed using automatic code generators.

During the visit to the Kurchatov Institute in Moscow, the panel learned of an effort to develop an engineering simulator for PWRs. However, this effort was in its initial phases, and little information was available at the time of the survey.

The Nuclear Plant Analyzer (NPA) is an engineering simulator developed at Idaho National Engineering Laboratory (Ref. 8.36). The desktop NPA is a microprocessor-based reactor transient simulation, visualization, and analysis tool. NPA aids an analyst in evaluating the transient behavior of nuclear plants by graphic displays. The desktop NPA integrated advanced reactor simulation codes with on-line computer graphics allows reactor plant transient simulation and graphical presentation of results. The graphics software is written in ANSI standard C and FORTRAN 77 and implemented over the UNIX/X-windows operating environment. The full interactive desktop NPA capabilities are now realized only with RELAP 5. RELAP 5 is a thermal-hydraulic code useful in simulating reactor coolant loops.

Summary of European Engineering Simulators

ANALYSIS

1. An active research effort exists in France to develop and enhance engineering simulators for use in the design and safety analysis of nuclear power plants.

2. A similar effort has been initiated in the Soviet Union.

COMPARISON

1. The Nuclear Plant Analyzer in the United States appears to be the equivalent of SIPA-2 in France.

EXTRAPOLATION

1. Because they are portable and flexible, additional uses will be made of workstation- and desktop-based engineering simulators. The addition of artificial intelligence such as expert systems to engineering simulators will lead to the creation of powerful on-line plant diagnostic systems that will be useful to control room personnel.

DATABASES

The panel tried to evaluate research on the use of databases in the European nuclear industry. Within the nuclear elements of the organizations surveyed, there were no research programs specifically on databases except in CEA France where research is undertaken to make available an experience feedback knowledge management tool called REX (Ref. 8.37). It is an object oriented database using semantic networks. Databases such as ORACLE and INGRES (developed by firms in the United States) were in use. Reference 8.38 describes the use of a large

database in an expert system, 3SE. This is a realtime expert system that aids an operator in monitoring all the electric power supplies in the 900 MWe PWR Bugey Unit 2 nuclear power plant in France. This system contains 150,000 pieces of data to describe over 12,000 components in the plant, and it uses the ORACLE database management system.

The panel found no standards or guidelines on the use of databases. From the discussions on databases, it seems the design issue in Europe is how best to use databases in local area networks and wide area networks. Also, as operating experience is obtained with the use of databases, guidelines and standards on their use will naturally develop. The use of databases in the European nuclear industry is about the same as that in the United States.

USER INTERFACE MANAGEMENT SYSTEMS

The survey of user interface management systems focused on graphics languages and interface tools and design techniques.

Graphics Languages And Interface Tools

The survey found that graphics languages were used to simplify the design of display formats. DATAVIEW, a graphics language developed in the United States, was used in the development of the interface for OASIS (Ref. 8.34), a workstation-based engineering simulator.

Another graphics language is PICASSO (Ref. 8.39). PICASSO is an integrated software package for the generation and execution of man-machine interface functions. It was developed at the Halden Reactor Project in Halden, Norway. PICASSO consists of two main modules: the off-line module and the on-line module. The off-line module consists of picture configuration tools:

1. An interactive graphics editor that is used to construct process pictures and to configure the operator's dialogue

2. An interactive database generator that is used to generate a local database for process variables

3. A documentation tool to describe the pictures, database content, etc., in readable text

The on-line module contains the tools used when the system is coupled to a realtime process or a simulator:

1. A display program for displaying the picture
2. A dialogue program for decoding and controlling operator dialogue
3. A station supervisor program for data exchange with other computers
4. A trend system for logging and displaying plant data

The ability to handle both static and dynamic picture information and to run the system with pictures and operator dialogue is the main difference between PICASSO and other graphics design tools.

OSF/MOTIF and Open Look (Ref. 8.40) are graphics tools often mentioned by the organizations surveyed in France, Germany, and the Soviet Union. These tool sets were developed and marketed by firms in the United States. In general, the surveyed organization was in the process of evaluating each of these graphics tool sets but had not made a decision on which one to select.

The status and use of graphics languages and interface tools in the U.S. nuclear industry are about the same as in Europe. Through informal conversations with personnel in the nuclear industry, this author learned that U.S. organizations are also in the process of evaluating OSF/MOTIF and Open Look.

Summary of Graphics Languages and Interface Tools Used in Europe

ANALYSIS

1. The European nuclear industry is actively using graphics languages and interface tools in the design of computer-driven interfaces.

COMPARISON

1. The nuclear industry in the United States is using similar graphics languages and interface tools in the design of computer-driven interfaces.

EXTRAPOLATION

1. The nuclear industry in the United States and in Europe will continue to make use of cost-effective, labor-saving interface design tools and products developed in the digital computer and software industry.

Design Techniques

A leading European researcher in human cognitive behavior is Dr. Jens Rasmussen of the RISO Laboratory, Denmark (Refs. 8.41-8.43). Rasmussen's model of cognitive behavior and his means-ends relational network are relevant to the design of nuclear power plant control room interfaces. Rasmussen classifies human cognitive behavior as skill-based, rule-based, and knowledge-based behavior.

Skill-based behavior is automatic; it requires no conscious effort on the part of the human. Upon perceiving an event, the human begins an automatic response. For example, upon seeing a reactor trip, a skilled operator will automatically strike the red manual trip button. A human acquires skill-based behavior by on-the-job training and by simulator training.

Rule-based behavior requires a conscious effort by humans. For example, when an operator finds that entry symptoms to a procedure are met, the procedure is executed. Study and practice is necessary to learn rule-based behavior. Skill-based behavior may be necessary to execute many of the steps in the procedure.

Knowledge-based behavior results from knowing and applying first principles. Examples of first principles are the conservation law for energy and for mass. Knowledge-based behavior is also hypothesis generation and testing. Another form of knowledge-based behavior is planning based on component and system performance.

Figure 8.5 presents Rasmussen's model of cognitive control in process systems. The model is complex, but it addresses a difficult problem. The attention surface presents data and information to the human in the form of displays. The data and information serve as input to the human's cognitive process of skill-, rule-, and knowledge-based behavior. The results from these various behavior types may be interaction with the action surface (skill-based behavior), an intention for actions (rule-based behavior), or a work plan (knowledge-based behavior). Human interaction with the action surface results in a manually initiated control action that affects the plant process. The human operator monitors the response of the plant through the attention surface.

The design of the attention surface must identify the data and information necessary for the human operator to evaluate the plant. In the process of evaluating the plant, the human cognitive effort may require skill-based behavior, rule-based behavior, and knowledge-based behavior. Instrumentation and data processing are necessary to gather and format the data for the attention surface.

The design of the action surface may contain keys, switches, mice, handles, and tracker balls. These devices permit the human to interact with control systems

and components in the plant. They are necessary to allow the human operator to execute assigned functions and tasks. Further, these devices may be necessary for operator intervention to mitigate consequences of unforeseen events. The design of the attention surface and the action surface should also account for operator errors and provide recovery means. In Reference 8.41, Rasmussen and Vicente identify, discuss, and analyze various human error types:

1. Errors related to learning and adaptation
2. Interference among competing cognitive control structures
3. Lack of resources
4. Intrinsic human variability

In discussing each of these types of errors, Rasmussen and Vicente also identify interface design guidelines (Ref. 8.41). The purpose of these guidelines is to increase the system's tolerance to human errors by providing the operator with improved means of controlling their effects on system performance.

A methodology that uses skill-based, rule-based, and knowledge-based behavior is cognitive diversity. Cognitive diversity maximizes human performance in the execution of complex functions and tasks. For example, if an operator is performing a critical task requiring skill-based behavior, the supervisor should verify the task by performing rule-based behavior. Similarly, if an operator is performing a critical task requiring rule-based behavior, the supervisor should verify the task by performing knowledge-based behavior. If the critical task requires knowledge-based behavior, no cognitive diversity is possible. The goal of cognitive diversity is to reduce common human mode error in performing critical functions and tasks. In its simplest form, cognitive diversity is the analog of hardware diversity, a design technique to defend against common mode hardware failures.

Effective support of human decision-making tasks requires decomposing the work domain (Ref. 8.42). The work domain consists of several levels of abstraction representing goals and requirements, abstract functions, general functions, physical functions, and the physical form. Rasmussen identifies this explicit formulation of the problem as the means-ends relational network. This appears to be the equivalent of the waterfall model used in the development of software, and it provides a top-level structure for designing the interface. The greatest detail exists at the physical form level, but this is the most difficult level to identify and solve problems because of the large quantity of data. Problem identification and solving at the goal level is easier, provided the detail at the physical form level has been mapped through the various levels of abstraction into goals.

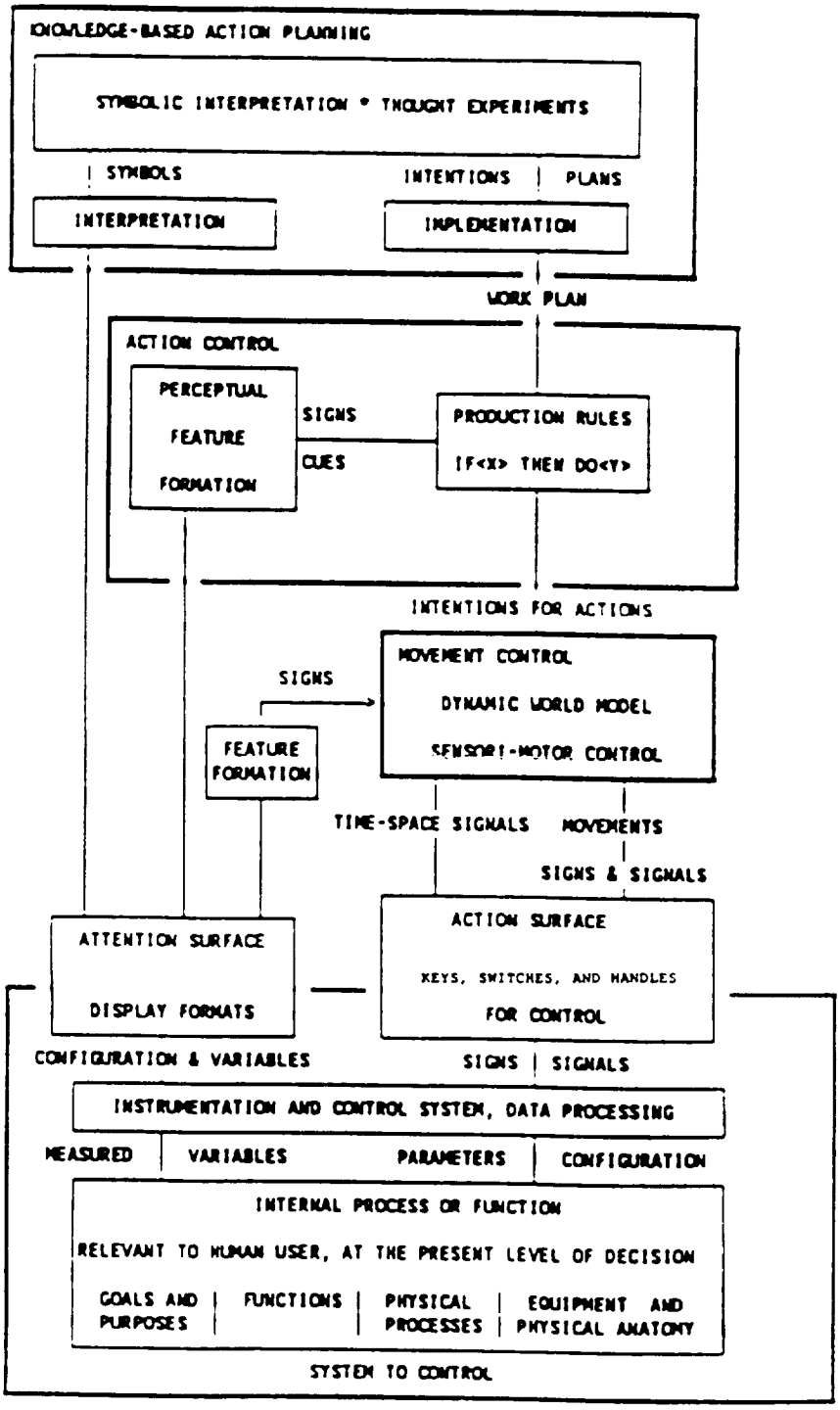


Figure 8.5. Rasmussen's Model of Cognitive Control for User Interfaces

Figure 8.6 is an illustration of the means-ends relational network as the top-level structure for designing an interface to monitor performance and energy in a typical nuclear power plant. This illustration identifies only the top-level structure. A considerable amount of work is necessary to identify and document the detail needed for interface design specifications. Further, feedback from the use of these design methods will provide the data necessary to fully evaluate their utility. Finally, Reference 8.44 presents one application of the means-ends relational network in a conceptual design of a display monitoring reactor coolant mass. Reference 8.45 contains another example of Rasmussen's taxonomy for human cognitive behavior in the U.S. nuclear industry.

European Designs for User Interfaces

Research on control room interfaces is under way at the Halden Reactor Project (Refs. 8.46-8.47). The ISACS-1 Program at Halden (Ref. 8.46) is a prototype of a computer-based integrated surveillance and control system. The goal of the ISACS-1 prototype is to act as a single integrated interface for the control room

GOAL:	Plant Performance
ABSTRACT FUNCTION:	Law of Conservation of Energy
GENERAL FUNCTION:	Energy Source, Energy Transport, Work, Energy Sink
PHYSICAL FUNCTION:	Reactor as Energy Source, Coolant Transports Energy Through Loops, Steam Turbine Work, Condenser Rejects Energy to the Environment Thermal Efficiency of Heat Engine.
PHYSICAL FORM:	Model-Based Displays, Mimics, Process Variables, System Variables, Procedures, Expert Systems as Decision Aids, Control Devices for Plant Components and Systems.

Figure 8.6. Use of Means-End Relational Network for Designing a User Interface

operator in all operational situations (normal, disturbance, accident). All information from the process and all commands to the process will pass through ISACS-1.

Many components within ISACS-1 are computerized operator support systems (COSSes). COSSes serve between the process instrumentation and the man-machine interface to refine process signals into information. Some COSSes use process modeling in which parts of the process are simulated in parallel to the plant process as an aid in monitoring the plant. Other COSSes utilize expert system methodology in diagnostic systems and operator advisory systems. A large number of COSSes have been developed and evaluated at Halden (Ref. 8.48). Other systems within ISACS-1 assist the operator in implementing manual controls.

To coordinate its many components, ISACS-1 uses an intelligent coordinator. The role of the intelligent coordinator is twofold:

1. Continuously supervise appropriate COSS analyses for the current plant situation, activate passive COSSes when necessary, and summarize and display plant status for the operator

2. When requested by the operator, coordinate additional assessments and report the results

In the supervisory role, the coordinator will prioritize and convey information from COSSes to the overview display. The operator may extract more detailed information in second-level displays that are maintained by the coordinator. Finally, the intelligent coordinator will propose detailed displays to the operator, either process display formats or special display formats relevant to the current plant state. In this context, the intelligent coordinator is performing the role of an interface management system.

Summary of User Interface Design Theory and Techniques in Europe

ANALYSIS

1. The cognitive control/process interface model appears useful.

2. The means-ends relational network provides a top-down interface design structure.

3. Prototype components of digital-computer-based control rooms are actively being evaluated at the Halden Reactor Project.

COMPARISON

1. The U.S. nuclear industry is making some use of the cognitive control/process interface model.

EXTRAPOLATION

1. Interface design methods will mature though operational feedback from operators using the interfaces.

CONCLUSIONS

The panel's analysis of the European nuclear industry's activity in software engineering, databases, and user interface management systems and the comparison with the activity in the United States may be summarized as follows.

Software Engineering

1. Europeans have developed and are actively using standards in the design of microprocessor-based nuclear power plant safety systems. Equivalent standards do not exist in the United States nuclear industry. However, activity is under way to develop equivalent standards.

2. Europeans are actively using CASE tools as aids in the design, development, and test of software for nuclear power plants. The use of CASE tools is much greater in Europe than in the United States.

3. Europeans have active research programs to evaluate the use of formal design methods to design and qualify safety critical software. Similar research programs exist in the United States but not in the nuclear industry.

4. Europeans have active programs to develop and use engineering simulators as tools for safety analyses and as design tools in the development of new nuclear power plants. A similar use of engineering simulators exists in the United States.

Databases

5. European use of databases in large expert systems is similar to that in the United States.

User Interface Management Systems

6. Europeans are using graphics languages in developing computer-driven interfaces. They are also evaluating interface design tools but have not yet selected a specific set for use. The U.S. nuclear industry's use of graphics languages and interface design tools is very similar to that in Europe.

7. The cognitive control/process interface model developed by Jens Rasmussen is applicable to nuclear power plant interfaces. Further, the means-ends relational network provides a structure to achieve top-down design of nuclear power plant interfaces. The U.S. nuclear industry is aware of both of these developments and is using elements of each.

Development Trends

8. Europe is clearly ahead in the use of CASE tools for the design and development of nuclear power plant software. Effective CASE tools for all phases of the software life cycle will result in high-quality software useful in nuclear power plants.

9. The use of databases as parts of information management systems and as parts of expert systems is relatively new. Operational experience and feedback are necessary to provide a basis for the development of guidelines and standards for database uses.

10. The use of graphic languages, interface design tools, and cognitive models for interface design is also relatively new. Operational experience and feedback are necessary to provide a basis for guideline and standards development.

11. Computer software is not easily scaled from the cathode-ray tube monitors that exist in today's control room to an all-digital control room. The development of a computer-based control room for a nuclear power plant will require a significant design and development effort.

REFERENCES

1. American National Standards Institute. "Criteria for Protection Systems for Nuclear Power Generating Stations." *IEEE Std 279-1971*, approved 5 April 1972.

2. Gimmy, K. L. "Operating Philosophy After 12 Reactor-Years Experience With On-Line Computers." American Nuclear Society Mtg, San Jose, PR, 1-3 Oct. 1969.

3. Gimmy, K. L. "Use of Digital Computers in the Protection System for Savannah River Reactors." American Nuclear Society Meeting on Thermal Reactor Safety, Sun Valley, Idaho, 1-4 August 1977.

4. Gimmy, K. L. and E. Nomm. "Automatic Diagnosis of Multiple Alarms for Reactor Control Rooms." American Nuclear Society Annual Meeting, Los Angeles, 6-11 June 1982.

5. Brown, E. M., W. J. Gill, S. R. Raktin, and W. T. Swain. "Validation of Safety System Software." International Atomic Energy Agency (IAEA) Specialist Meeting on Software Reliability for Computerized Control and Safety in Nuclear Power Plants, Pittsburgh, 20-22 July 1977.

6. U.S. Nuclear Regulatory Commission. "Safety Evaluation Report Related to Operation of Arkansas Nuclear One, Unit 2." *NUREG-0308*, Docket No. 50-368. November 1977.

7. U.S. Nuclear Regulatory Commission. "Safety Evaluation Report Related to Operation of Arkansas Nuclear One, Unit 2." *NUREG-0308*, Docket No. 50-368, Supplement Number 1. June 1978.

8. U.S. Nuclear Regulatory Commission. "Safety Evaluation Report related to Operation of Arkansas Nuclear One, Unit 2." *NUREG-0308*, Docket No. 50-368, Supplement Number 2. September 1978.

9. Beltracchi, L. and J.B. Bullock. "Safety Evaluation Experience with Digital Computer Software," *Nuclear Safety 17* (no.6, November-December 1976).

10. Naventi, R. "Documentation of Safety Software Systems for Reliability and Qualification." IAEA Meeting on Software Reliability for Computerized Control and Safety in Nuclear Power Plants, Pittsburgh, 20-22 July 1977.

11. American National Standards Institute. "Application Criteria for Programmable Digital Computer Systems in Safety Systems on Nuclear Power Generating Stations." *ANSI/IEEE-ANS-7-4.3.2-1982.* Approved 6 July 1982.

12. U.S. Nuclear Regulatory Commission. "Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants." *Regulatory Guide 1.152.* USNRC, Office of Nuclear Regulatory Research. (U.S. Government Printing Office, PO Box 37082, Washington, DC 20013-7082.)

13. Redmill, F. J. "Dependability of Critical Computer Systems 2." In *Guidelines produced by The European Workshop on Industrial Computer Systems, Technical Committee 7* (EWICS TC7). New York:Elsevier Applied Science, 1988.

14. International Electrotechnical Commission. "Software for Computers in the Safety Systems of Nuclear Power Plants." *Standard 880,* 1986.

15. Pilaud, E. "Development and Qualification of Core Protection and Control System 'CO3' For N4 Type Reactors." Merlin Gerin, Safety Electronic Systems Dept.

16. Ministry of Defence. "Requirements for the Procurement of Safety Critical Software in Defence Equipment." *Interim Defence Standard 00-55.* U.K., May 1988.

17. Miles, J. B. "4GLs and CASE." *Government Computer News* p 49 (7 Jan. 1991).

18. Bergerand, J. L. and E. Pilaud. "SAGA: A Software Development Environment For Dependability Automatic Controls." Merlin Gerin usine M4, 38050 Grenoble, Cedex, France.

19. Pilaud, E. See Ref. 8.15.

20. Lapassat, A. "Real Time Systems Software Validation and Verification." International Logistics Engineering Seminar, Dubrovnick, Yugoslavia, 19 Aug. 1987.

21. Personal communication with Dr. Arnold Graf, KWU, Germany, 29 Nov. 1990.

22. Dahll, G. and J. E. Sjoberg. "SOSAT--A Set of Tools for Software Safety Assessment." Second European Conference on Software Quality Assurance, Oslo, Norway, 30 May-1 June 1990.

23. Halstead, M. H. *Elements of Software Science.* New York:Elsevier, North Holland Publ. Co., 1977.

24. Gorlin, A. and S. Semenov. "Range of Expert Systems For Control, Modeling, and Safety Operation in Nuclear Energy." Specialists' Meeting on Artificial Intelligence in Nuclear Power Plants, Helsinki, 10-12 October 1989.

25. Boehm, B. W. "A Spiral Model of Software Development and Enhancement." *Computer* pp 61-72 (May 1988).

26. Personal communication with Dr. F. Saglietti, GRS Garching, 1 Dec. 1990.

27. Saglietti, F. "Strategies for the Achievement and Assessment of Software Fault-Tolerance." 11th IFAC World Congress, Automatic Control in the Service of Mankind, Tallin, Estonia, USSR, 13-17 August 1990.

28. Saglietti, F. "Software Diversity Metrics Quantifying Dissimilarity in the Input Partition." *Software Engineering Journal 5* (no. 1, January 1990).

29. Saglietti, F. "The Impact of Voter Granularity in Fault Tolerant Software on System Reliability and Availability." Fault Tolerant Computing Systems, Automation Systems, Methods, Application, 4th International GI/ITG/GMA Conference, Baden-Baden, Germany, 20-22 September 1989.

30. Saglietti, F. "Optimal Combination of Software Testing Strategies." *Safety of Computer Control Systems 1988, Proceedings of the IFAC Symposium*, Fulda, Germany, 9-11 November 1988.

31. Dahll, G., M. Barnes, and P. Bishop. "Software Diversity--A Way to Enhance Safety?" Second European Conference on Software Quality Assurance, Oslo, Norway, 30 May-1 June 1990.

32. Dahll, G. "Software Specifications--The Requirement." ESRRDA Seminar on Software Reliability, Brussels, Belgium, 14 September 1988.

33. Dufour, P. "OASIS: An Interactive Simulation Tool For Safety Analysis." Commissariat à l'Énergie Atomique (CEA), Centre de Cadarache, 13108 Saint Paul Lez Durance, Cedex, France.

34. Dufour, P., J-P Doat, B. Papin, and C. Pauwells. "OASIS And CORIANDRE: User Friendly And Flexible Simulation Tools For FBR's And PWR's Transient Analysis." CEA, Centre de Cadarache, Cedex, France.

35. Personal communication with Dr. Jean Peltier, CEA Institut de Protection et de Sûreté Nucléaire, 27 November 1990.

36. Beelman, R. J. "Nuclear Plant Analyzer Desktop Workstation." Water Reactor Safety Meeting, Rockville, Maryland, October 1990.

37. IAEA/NEA Specialist Meeting on Tools for Experience Feedback Management, Vienna, Austria, May 14-19, 1990.

38. Ancelin, J., F. Cheriaux, J. P. Gaussot, D. Pichot, G. Sancerni, and G. Voisn. "Expert System Monitoring Electric Power Supplies Bugey Nuclear Power Plant." EDF Research and Development Division, 6 Quai Waiter, 78400 Chatou, France.

39. Owre, F. and S. Nilsen. "Integration Of A Real Time Expert System And A Modern Graphic Display System In A Swedish Nuclear Power Plant Control Room." *Expert Systems With Applications*, December 1990.

40. Wilson, C. "Gettin GUI." *Workstation News*, p 28 (November, 1990).

41. Rasmussen, J. and K. Vicente. "Cognitive Control Of Human Activities And Errors: Implications For Ecological Interface Design." Fourth International Conference on Event Perception and Action, Trieste, Italy, 24-28 August 1987.

42. Rasmussen, J. and L. P. Goodstein. "Information Technology and Work." Chapter 9 in *Handbook of Human-Computer Interaction*, ed. M. Helander. New York:Elsevier Science Publishers, 1988.

43. Rasmussen, J. and K. Vicente. "Coping With Human Errors Through System Design: Implications For Ecological Interface Design." *International Journal of Man-Machine Studies* 431:517-34 (1989).

44. Beltracchi, L. "Conceptual Design Of A Computer-Driven Display For Monitoring Reactor Coolant Mass." Accepted for publication in the June 1991 issue of *The IEEE Transactions On Nuclear Science.*

45. Cheng, J. F., R. Chaing, C.C. Yao, A. J. Spurgin, D. D. Orvis, B. K. H. Sun, D. G. Cain, and C. Christensen. "Evaluation Of An Emergency Operating Procedure Tracking Expert System By Control Room Operators." Expert Systems Applications For The Electric Power Industry, Orlando, Florida, 6-8 June 1989.

46. Haugset, K., O. Berg, J. K. Fordestrommen, and W. R. Nelson. "ISACS-1, The Prototype Of An Advanced Control Room." International Symposium On Balancing Automation And Human Action In Nuclear Power Plants, Munich, 9-13 July 1990.

47. Krogsaeter, M., J. S. Larsen, S. Nilsen, and F. Owre. "The Computerized Procedure System COPMA and its User Interface." International Atomic Energy Agency Specialist Meeting on Artificial Intelligence in Nuclear Power Plants, Helsinski, Finland, 10-12 October 1989.

48. Haugset, K., O. Berg, T. Bjorlo, O. Evjen, and N. T. Fordestrommen. "ISACS--An Integrated Surveillance And Control System For The Advanced Control Room." IEEE Fourth Conference On Human Factors And Power Plants, Monterey, CA, 5-9 June 1988.

APPENDIX 8.A

TECHNOLOGY AREA: STANDARDS/TOOLS

The Technology Area of Standards and Tools consists of the following topics:

Software Engineering

Data Bases

User Interface Management Systems

The following survey questions are for the commercial nuclear power industry in the country surveyed:

SOFTWARE ENGINEERING

Safety System Software Standards

What standards are used in the design, development, and acceptance of critical software for nuclear power plants? (Critical software executes safety functions such as tripping the reactor, initiating engineered safeguard systems.)

Digital Process Control System Software Standards

What standards are used in the design, development, and acceptance of digital process control systems and computer-driven display systems for monitoring the plant?

Quality Assurance Standards

What are the quality assurance standards required in the design and development of software? Are there research programs under way/planned for the development of quality assurance methods and techniques?

Software Life Cycle

Does the nuclear industry in your country require the use of a software life cycle in the development of computer programs? If yes, what is the life cycle?

Computer Language Standard

Does your country require the use of a standard computer language in your nuclear power plants? If yes, identify the language and the reason for its choice. Is there a research program for the development of a standard language? If yes, provide details on the program.

Formal Methods

Are formal methods required in the design and development of computer programs used in the nuclear industry? If yes, what are the formal methods? Are there any research programs under way/planned for the evaluation of formal methods in software engineering?

Program Generators

Are program generators used for the development of computer code used in nuclear power plants? If yes, what were the reasons for choosing the generator? Are there any research programs under way/planned for the development of program generators?

Tools

What tools, if any, exist to aid in the verification of design and coding of the computer programs? Are there any research programs under way/planned for the development of verification tools?

Configuration Control

What standards and tools are used in configuration control during the design and development of software?

Scope of Software Testing

Does the testing and validation of software require structural, functional, and statistical evaluations? Is research under way/planned for the development of methods, techniques, and tools for structural, functional, and statistical evaluations? If yes, what are they?

Metrics

Are metrics used in the design, development, and test of the computer code? If yes, define the metrics. Are there any research programs under way/planned for the development and use of metrics? If yes, what are they?

Software Reliability

Does your country require any reliability standards prior to the use of software in a nuclear power plant? If yes, what are they? Are there any research programs under way/planned for the development of reliability methods and techniques?

Software Tools

What type of computer aided software engineering tools are available for the design, development, test, and documentation of software? Are there any research programs under way/planned for the development of computer aided software engineering tools?

Fault Tolerance, Fault Avoidance

What are the requirements for fault tolerance/fault avoidance methods and techniques for computers used in nuclear power plants? Are there any research programs under way/planned for the development of fault tolerant/fault avoidance techniques?

Common Mode Fault Defenses

What are the defenses against common mode faults in critical software, such as software used in safety systems? Is the use of functional diversity a required defense against common mode software errors? Are there any research programs under way/planned for the development of defenses against common mode faults in software?

Documentation Standards

What are the standards for the documentation of software used in nuclear power plants? When does documentation occur in the software life cycle? Are there any research programs under way/planned for the development of documentation standards?

Software Maintenance Standards

What are the standards on the maintenance of software? Are there any research programs under way/planned for the development of standards for software maintenance?

Software Retirement/Replacement

Do any standards exist for the retirement/replacement of software? What are the requirements for the retirement/replacement of software? Are there any research programs under way/planned for the development of standards for the retirement/replacement of software?

Expert System Development Tools

Has your country standardized on tools for the development of expert systems? Neural networks? Are there any research programs under way/planned for the development of such tools and standards?

Object Oriented Programming

Do any standards exist for the use of object oriented programming? Are there any research programs under way/planned for the development of object-oriented programming tools?

Defense - Viruses & Bugs

What tools are you using to defend against viruses and bugs? Are there any research programs under way/planned for the development of such tools?

DATA BASES

Data Base Standards

What standards exist on data bases for nuclear power plants? Have your nuclear power plants standardized on the use of a specific data base? If yes, what are the name and characteristics of the data base?

Data Base Design Tools

What tools exist for the design, development, and use of data bases?

Data Base Development Tools

What research is under way/planned for the development of data bases and data base tools?

Report Generators

Are report generators used with data bases? Is research under way/planned for the development of report generators?

Query Languages

Are query languages and view formats used with data bases? Is research under way/planned for the development of query languages and view formats?

Data Entry Templates and Screens

Are entry templates/screen formats used for data entry to data bases? Is research under way/planned for the development of entry templates/screen formats?

Graphic Interfaces

Are graphic user interfaces used for working with data bases? Is research under way/planned for the development of graphic user interfaces?

Tutorials

Are tutorials available for use in learning how to use the data base? Is research under way/planned for the development of tutorials?

Networked Data Bases

Are data bases interconnected by means of a network? What tools exist for use of the data bases on a network? Is research under way/planned for the development of networks and tools for using data bases on networks?

Information Models

In the design of data bases, how are information models used in the design process? Is there any research under way/planned for the development of information models for service in the design process?

Tools for Consistency Checks

What tools are used to check information for consistency and completeness in data bases? Is there any research under way/planned for the development of tools to check information for consistency and completeness?

Security

What tools exist to maintain the security of data bases? Is there any research under way/planned for the development of tools to maintain the security of a data base?

Relational Data Bases

Are the data bases in your power plants relational? What standards exist for the use of relational data bases? Is there any research under way/planned for the development of relational data bases and of standards for their use?

Functional Applications

What are the functional applications of data bases in your nuclear power plants? Is there any research under way/planned for the development of new applications of data bases in your nuclear power plants?

USER INTERFACE MANAGEMENT SYSTEM:

Software Development Tools

What tools are used for the development of application programs for nuclear power plants? Is there any research under way/planned for the development of tools?

User Interface Development Tools

What tools are used for the development of display formats for use in nuclear power plants? Is there any research under way/planned for the development of tools to aid in the development of display formats? A user interface management system?

Windows

Are standards and guidelines available in the use of windows for interface design? Is there any research under way/planned for the development of window design tools?

Graphics Language

Has a graphics language been adopted as a standard/guideline for the design and development of interfaces? Is a graphics editor used for development and maintenance of display formats? Is there any research under way/planned for the selection of a graphics language as a standard?

Menus

Does a menu standard or guideline exist for interface design? Is there any research under way/planned for the development of such a standard or guideline?

OSF/Motif

Is the OSF/Motif toolkit used in the design and development of interfaces? Is there any research under way/planned for the selection and use of toolkits for interface design? If yes, what are the key factors in the selection process?

APPENDICES

A. PROFESSIONAL EXPERIENCE OF PANEL MEMBERS

James D. White (Co-Chairman)

LWR and LMR Programs
Oak Ridge National Laboratory
Bldg 3500, Mail Stop 6009
P.O. Box - 2008
Oak Ridge, TN 37831 - 6009

James White is currently technical director of Light Water Reactor and Liquid Metal Reactor Programs of Oak Ridge National Laboratory. He has worked as a nuclear engineer for ORNL for twenty-five years. At the time this study was initiated, Mr. White was manager of the advanced controls program at ORNL, studying the application of advanced computer architecture, advanced control theory, artificial intelligence and advances in man-machine interfaces to the control of advanced reactors. Previously, Mr. White has managed programs in transient rod bundle heat transfer, pressurized thermal stock, assessment of market viability of advanced reactor concepts, software engineering and information engineering. Mr. White received B.S. and M.S. degrees in Nuclear Engineering from the University of Tennessee in 1977 and 1978.

David D. Lanning (Co-Chairman)

MIT
Department of Nuclear Engineering
77 Massachusetts Ave., Rm. 24-212
Cambridge, MA 02139

David Lanning is a Professor of Nuclear Engineering at the Massachusetts Institute of Technology. He has been a consultant to a number of firms in the electric utility and nuclear industries, including Stone and Webster Engineering Corporation, Northern States Power, Boston Edison, and GA Technologies. His professional interests include nuclear engineering education and the design, safety,

control, and operation of nuclear reactor systems. In the 1950s, he worked for General Electric at Hanford and in the 1960s for Battelle Northwest Laboratories. At MIT during the 1970s, he was Co-Director in charge of the MIT Reactor, with responsibility for the design and installation of the MITR-II. He has also been a co-principal investigator of MIT's Program on Nuclear Power Plant Innovation in the area of modular high-temperature gas-cooled reactors (MHTGR), and he is also the group coordinator for the Advanced Instrumentation and Control Program in the MIT Nuclear Engineering Department. In conjunction with his teaching and research at MIT, he is presently a member of the MIT Reactor Safeguards Committee and a member of the Steering Committee for the NASA-sponsored MIT Space Grant Program. Also, he is the graduate student Financial Aid Officer for the Nuclear Engineering Department. In addition to consulting on utility safety audit committees, he served on the National Academy of Sciences/National Research Council's Committee to Assess Safety and Technical Issues at DOE (Department of Energy) Reactors, which was active August 1986 to July 1988.

Leo Beltracchi

U.S. Nuclear Regulatory Commission
5640 Nicholson Lane
MS-NLN 316
Rockville, MD 20852

Leo Beltracchi is a member of the research staff at the U.S. Nuclear Regulatory Commission. His current projects address the development of guidelines for verifying and validating expert systems and the development of assessment methods to evaluate computer-driven interfaces. In a previous assignment, he led a team of engineers in the safety evaluation of a reactor trip system containing a digital computer. Subsequent to the Three-Mile Island accident, he served on the Commission's "Lessons Learned Task Force" and originated the "Safety Parameter Display System."

Prior to joining the NRC in 1974, Mr. Beltracchi's work experience consisted of the design and development of a computer-driven terminal air traffic control system, the design and test of scientific software, and the analysis and design of control systems for nuclear power plants.

Frederick R. Best

Nuclear Engineering Dept.
Zachary Engineering Center
Room 129
Texas A&M University
College Station, TX 77843-3133

Frederick Best is an Associate Professor at Texas A & M University in the Nuclear Engineering Department. During the 1980s Mr. Best worked on several research projects including heat and mass transfer modeling for spent fuel pool analysis, for Sandia National Laboratories, and LOCA Mitigation SP-100 Space Reactor System, for General Electric.

Mr. Best received his B.M.E. degree in Mechanical Engineering in 1968 from Manhattan College. He received his S.M. degree and Ph.D. in Nuclear Engineering in 1970 and 1980; both of these degrees are from the Massachusetts Institute of Technology.

James R. Easter

Westinghouse Energy Center
Northern Pike Blvd.
Monroeville, PA 15146
BAY 457 East

James Easter has been employed with the commercial nuclear power divisions of Westinghouse for 26 years. He began his career at Westinghouse working on the nuclear core design of the Southern California Edison San Onofre Nuclear Generating Station and continued in the nuclear core design area for 10 years, working on subsequent core designs and developing methods for analyzing, controlling, and monitoring core power distribution. The next five years he spent working on the core power distribution monitoring aspects of the development of the Westinghouse Digital Integrated Protection System. An interest in improving the operator understanding of the results of such a system led to working on the development of a new, digital advanced control room. The last 10 years, Mr. Easter has spent developing an understanding of the role an operator has in the control room, the tasks that he must perform, and in developing appropriate computer based interfaces to help him do his job in a more effective and error-free way. Mr. Easter holds a B.S. degree in mechanical engineering from Stanford University and a M.S. degree in nuclear engineering from the University of Virginia.

Lester C. Oakes

5016 Mountaincrest Dr.
Knoxville, TN 37918

Lester Oakes is on assignment with the Electric Power Research Institute, helping to develop a strategy for upgrading commercial power reactor instrumentation and control systems. He began his career developing and applying analog computers to simulate the dynamic response of nuclear reactors to aid in the design of high performance control and plant protection systems. He has received a number of patents, including one for the automatic startup of a nuclear reactor. He has served as the Associate Division Director of the Instrumentation and Control Division and Head of the Reactor Systems Section of ORNL. He is a Fellow of the Institute of Electrical and Electronic Engineers, and was named Outstanding Engineering Alumnus at the University of Tennessee in 1984.

Mr. Oakes was awarded his B.S. degree in Electrical Engineering in 1949 and his M.S. degree in 1962, both by the University of Tennessee.

A. L. Sudduth

Duke Power Company
P.O. Box 1006
526 S. Church Street
Charlotte, N.C. 28201-1006

A. L. Sudduth is an Engineering Consultant with Duke Power Company in Charlotte, NC. His current responsibilities include the upgrading of instrumentation and control systems in fossil-fueled power stations and the development of training simulators. He has over 15 years experience in the nuclear industry and is a recognized utility industry expert on applications of Artificial Intelligence in the operation of power plants.

Mr. Sudduth holds M.S. degrees in Electrical and Mechanical Engineering. He is a member of ASME, a senior member of IEEE, and a registered professional engineer.

B. GLOSSARY

BRS	Boron Concentration Adjustment Control System
CE	Combustion Engineering
CEA	Cadarache Research Center
CO3	Core Instrumentation and Control for the N-4 Control Room
CPC	Core Protection Calculation
DNBR	Departure from Nuclear boiling Ratio
FW	Feedwater
NPP	Nuclear Power Plant
N-4 PWR	Next Generation of French PWR Plants 1,475 MWe (CHOOZ B1 is the first plant)
P-20	"Controbloc" System for the N-4 Control Room
PCI	Pellet-clad Interaction
PWR	Pressurized Water Reactor
S3C	Simulator for the N-4 French PWR "Computerized Control Room" System
Siemens KWU	Siemens Power Generation Group
SG	Steam Generator
SPIN	French Digital Reactor Protection System
VVER	Russian-designed Pressurized Water Reactor

BIBLIOGRAPHY

Adamov, E. O., Gavrilov, P. A., Gorelov, A. I., Ephanov, A. I., Michailov, M. N., Sazonov, N. A., "An Automated Data System for the Monitoring of RBMK-1500 Reactors: Status and Potential," IAEA-CN-49/98.

Adler, P., "New Technologies, New Skills", *California Management Review,* Volume XXIX, No. 1, Fall, (1986).

Aleite, W., "Computer Applications For Nuclear Power Plant Operation and Control in the FRG," ANS Topical Meeting, Pasco, WA, Sept. 8-12, 1983.

Aleite, W., "PRISCA: KWU's New NPP Process Information System," *Nuclear Europe*, p 24-26 Oct. 1989.

Aleite, W., "Full Load-Follow Capability of KWU PWR NPP by Full Automatic Power Control," IFAC Symposium, Beijing 12./15. August 1986, Power System and Control.

Aleite, W., "Remarks about 'Why' and 'How' of KWU Konvoi PRINS," IAEA Specialists Meeting on Operational Experience with Control and Instrumentation Systems in Nuclear Power Plants, Brussels, Belgium, November, 1987.

Ancelin, J., Cheriaux, F., Gaussot, J.P., Pichot, D., Sancerni, G., and Voisn, G., "Expert System Monitoring Electric Power Supplies Bugey Nuclear Power Plant," Electricite de France Research and Development Division, 6, quai Waiter, 78400 Chatou, France

Ancelin, J., J. P. Gaussot, M. Gondran, and P. Legaud, "EXTRA: a Real Time Knowledge Based Monitoring System for a Nuclear Power Plant," *Proceedings of Man Machine Interface in the Nuclear Industry*, IAEA-CN-49/66, Vienna, 1988.

ANSI/IEEE-ANS-7-4.3.2-1982, "Application Criteria for Programmable Digital Computer Systems in Safety Systems on Nuclear Power Generating Stations," Approved July 6, 1982, by the American National Standards Institute.

Aschenbrenner, J.F., Colling, J.M., Raimondo, E., "Reactor Instrumentation and Control For the French N4 Nuclear Power Plants Units," IAEA-Microprocessors in Systems Important to the Safety of Nuclear Power Plants, London, U.K., May 10-12, 1988.

Aviles, B. N., "Digital Control Strategies for Spatially-Dependent Reactor Cores with Thermal-Hydraulic Feedback," Ph.D. Thesis, Department of Nuclear Engineering, Massachusetts Institute of Technology, Cambridge, MA, February 1990.

Bastl, W., H. Schuller, and D. Wach, "High Performance and Safety of Nuclear Power Plants by Means of Early Fault Detection," *Man-Machine Interface in the Nuclear Power Industry*, IEAE-CN-49/4, pp. 305-322, 1988.

Bastl, W. and H. Markl, "The Key Role of Advanced Man-Machine Systems for Future Nuclear Power Stations," IAEA-CN-49/56, presented at the conference on Man-Machine Interface in the Nuclear Industry, Vienna, 1988.

Beelman, R.J., "Nuclear Plant Analyzer Desktop Workstation," Water Reactor Safety Meeting, Rockville, Maryland, October, 1990.

Beltracchi, L., "Conceptual Design Of A Computer-Driven Display For Monitoring Reactor Coolant Mass," accepted for publication in the June 1991 issue of The *IEEE Transactions On Nuclear Science.*

Beltracchi, L. and Bullock, J.B., "Safety Evaluation Experience with Digital Computer Software," *Nuclear Safety,* Vol. 17, No.6, November-December, 1976.

Berg, O., and M. Yokobayashi, "Combination of Numeric and Symbolic Processing in Fault Detection and Diagnosis," Halden Report HWR-174, March, 1986.

Bergerand, J.L., "A Global Approach For Software Design In A Dependable Context," International Working Group--Nuclear Power Plant Control and Instrumentation, Lyon, France, April 1990.

Bergerand, J.L., and Pilaud, E., "SAGA: A Software Development Environment For Dependability Automatic Controls," Merlin Gerin usine M4, 38050 Grenoble, Cedex, France.

Bock, H. W., "Future Main Control Room Design for Siemens Nuclear Power Plants," IAEA-CN-49/28.

Boehm, B.W., "A Spiral Model of Software Development and Enhancement," *Computer,* May 1988, pgs 61-72.

Bohr, E., "Design of Nuclear Power Plant Control Rooms: Some Findings and Possible Improvements", in *Operational Safety of Nuclear Power Plants, Proceedings of an International Symposium,* pgs. 221-229 Vol. 1, (1984).

Breuzè, G., Serre, J., "Fiber Optic Components Compatibility with the PWR Containment Radiation Field", IAEA Specialists' Meeting on Communication And Data Transfer in Nuclear Power Plants, 24-26 April, 1990, Lyon, France.

"British Support French I&C System that EDF has Abandoned for Its N4," *Nucleonics Week,* Jan. 10, 1991.

Brown, E.M., Gill, W.J., Raktin, S.R., and Swain, W.T., "Validation of Safety System Software," International Atomic Energy Agency Specialist Meeting on Software Reliability for Computerized Control and Safety in Nuclear Power Plants, Pittsburgh, Pennsylvania, July 20-22, 1977.

Buner, D., Pashchenko, F. F., Kolev, N. P., Tsvetanov, R., "Adaptive Algorithms for VVER REactor Core Surveillance," *Modelling Simulation and Control,* AMSE Press, Vol. 18, No. 1, pp. 19-30.

Burel, J-P., Ringeard, C., "A New Design For Experimental reactors Digital Nuclear Instrumentation System," Specialists Meeting on Microprocessors in Systems Important to Safety of Nuclear Power Plants, London, United Kingdom, May 10-21, 1988.

Chachko, S. A., "Ways of Preventing Errors by the Operating Personnel of Nuclear Power Stations", in *Elektr. Stantsii* (U.S.S.R.) No. 3, pgs. 6-10, (1987).

Cheng, J.F., Chaing, R., Yao, C.C., Spurgin, A.J., Orvis, D.D., Sun, B.K.H., Cain, D.G., and Christensen, C., "Evaluation Of An Emergency Operating Procedure Tracking Expert System By Control Room Operators," Expert Systems Applications For The Electric Power Industry, Orlando, Florida, June 6-8, 1989.

Combe, M., Personal communication," Evolution of Operating System for Electronuclear Power Plants at EDF," November 28, 1990.

Dahll, G. and Sjoberg, J.E., "SOSAT--A Set of Tools for Software Safety Assessment," Second European Conference on Software Quality Assurance, Oslo, Norway, May 30-June 1,

Dahll, G., Barnes, M., and Bishop, P., "Software Diversity--A Way to Enhance Safety?", Second European Conference on Software Quality Assurance, Oslo, Norway, May 30-June 1, 1990.

Dahll, G., "Software Specifications--The Requirement," ESRRDA Seminar on Software Reliability, Brussels, Belgium, September 14, 1988.

Druschel, R. Maier, W. Schramm, W., "Modernization of I&C Systems in Nuclear Power Plants," European Nuclear Conference, Lyon, France, Sept. 23-28, 1990.

Dufour, P., Doat, J-P., Papin, B., and Pauwells, C., "OASIS And CORIANDRE: User Friendly And Flexible Simulation Tools For FBR's And PWR's Transient Analysis," Commissariat a l'Energie Atomique CEA, Centre de Cadarche, 13108 Saint Paul Lez Durance CEDEX - France.

Dufour, P., "OASIS: An Interactive Simulation Tool For Safety Analysis," Commissariat a l'Energie Atomique CEA, Centre de CADARCHE, 13108 Saint Paul Lez Durance CEDEX - France.

Elzer, P., Weisang, C., Zinser, K., "Knowledge-Based System Support for Operator Tasks in S&C Environments", Proceedings of the 1989 International Meeting on Systems, Man, and Cybernetics, Boston, Mass., (1989).

Elzer, P., Siebert, H., Zinser, K., "New Possibilities for the Presentation of Process Information in Industrial Control", Third IFAC/IFIP/IEA/IFORS Conference, Oulu, Finland, 14-16 June 1988, International Federation of Automatic Control, (1988A).

Elzer, P., Borchers, H. W., Weisang, C., and Zinser, K., "Knowledge-Supported Generation of Control Room Pictures", Proceedings of the IFAC Workshop, Clyne Castle, Swansea, UK, 21-23 September 1988, International Federation of Automatic Control, (1988B).

Endrizzi, I., Wenndorff, C., "PDD and Aeroball Improve Flexibility," *Nuclear Engineering International*, Vol. 34, No. 435, Dec. 1989.

Felkel, L., Dipl.-Inform., Information Concepts Subsection, Systems Division, Gessellschaft fur Reaktorsicherheit (GRS) mbH, Reactor Safety Company Ltd., Forschungsgelaende, D-8046 Garching, Germany (personal communication).

Felkel, L., "The STAR Concept, Systems to Assist the Operator During Abnormal Events", *Atomkernenerg. Kerntech.* (Germany) Vol. 45, No. 4, pgs. 252-260, December, (1984).

Fiber Optics Workshop, Proceedings of Electric Power Research Institute Report, EPRI ER-6537, 1989.

Fischer, H. D., et al., "Digital Information and Control System for Non-safety and Safety Applications in Nuclear Power Plants of the 1990's," Paper presented at European Nuclear Conference in Lyon, France, Sept. 23-28, 1990.

"Force EDF to Abandon I&C System for N4", *Nucleonics Week*, Vol. 32, No. 1, Jan. 3, 1991.

Framatome Group, "Experience Feedback after Six Years of Load Following Operations," 1990 Brochure.

Frederick, E. R., "Design, Training, Operations--The Critical Links, An Operator's Perspective", IAEA-SM-296/91, International Symposium on Severe Accidents in Nuclear Power Plants, Sorrento, Italy, pgs. 21-25, March, (1988).

Furet, J., Chef De Service, Instrumentation et Systems Nucleaires, Centre D'Etudes Nucleaires De Saclay, F 91191 Gif-Sur-Yvette, Cedex, France (personal communication).

Gallagher, J. M., *Disturbance Analysis and Surveillance System Scoping and Feasibility Study,* EPRI NP-2240, July, 1982.

Gimmy, K.L. and Nomm, E., "Automatic Diagnosis of Multiple Alarms for Reactor Control Rooms," American Nuclear Society Annual Meeting, Los Angeles, California, June 6-11, 1982.

Gimmy, K.L., "Operating Philosophy After 12 Reactor-Years Experience With On-Line Computers," American Nuclear Society Meeting, San Jose, Puerto Rico, October 1-3, 1969.

Gimmy, K.L. "Use of Digital Computers in the Protection System for Savannah River Reactors," American Nuclear Society Meeting on Thermal Reactor Safety," Sun Valley, Idaho, August 1-4, 1977.

Gmeiner, L., "Microprocessor-Based Integrated LMFBR Core Surveillance", Institut fur Datenverarbeitung in der Technik Projekt Schneller Bruter, June 1984.

Gonchukov, Podkolzina, (VNIIAES), "Evaluation of Sources of Operator Misfunctions and Mistakes for VVER-1000 NPPs", personal presentation at the Kurchatov Institute, Moscow, U.S.S.R., December, (1990).

Gorlin, A., A. Polyakov, and S. Semenov, "Some Applications of AI Technology in Nuclear Industry," IAEA Demonstration of Expert Systems Technology which took place in Moscow October 1-5, 1990.

Gorlin, A. and Semenov, S., "Range of Expert Systems for Control, Modeling, and Safety Operation in Nuclear Energy." Paper given to the panel on the visit to Moscow 12/4/90.

Guesnier, G., Anglaret, M., Collings, J.M., Raimondo, E., "Control and Instrumentation Systems for France's N4 NPPs," *Nuclear Europe*, Vol. IX, No. 1, Sept. 1989.

Guesnier, M.G., "An Entirely Computerized Control Room for the N4 PWR," *Nuclear Engineering International*, Vol. 32, No. 394, May 1987.

Halstead, M.H., *Elements of Software Science,* Elsevier, North Holland Publ. Co., NY 1977.

Hamelin, J.F., "OSI Industrial Networking at Electricite De France, Electricite' de France, Direction des Etudes et Recherches, 6, Quai Waiter, 78401 Chatou CEDEX France.

Hansen, K. F., Evans, E. A., Behnke, W. B., Olander, D. R., Cousin, S. B., White, J. D., Ransom, V. H., *JTEC Panel Report on Nuclear Power in Japan,* the National Science Foundation and the Department of Energy of the United States Government, (1990).

Haugset, K., Berg, O. Bjorlo, T., Evjen, O. and Fordestrommen, N.T., "ISACS--An Integrated Surveillance And Control System For The Advanced Control Room," IEEE Fourth Conference On Human Factors And Power Plants, Monterey, CA, June 5-9, 1988.

Haugset, K., Berg, O., Fordestrommen, J. K., Nelson, W. R., "ISACS-1, The Prototype of an Advanced Control Room", IAEA-SM-315/16, International Symposium on Balancing Automation and Human Action in Nuclear Power Plants, Munich, Federal Republic of Germany, pgs. 9-13, July, (1990).

Helander, M. (Ed.), *Handbook of Human-Computer Interaction*, Elsevier Science Publishing Co., Inc., (1988).

Hoffman, H., Fischer, H. D., Lochner, K.H., Mertens, U., "Digital Information and Control Systems," paper presented at the Poster Session during the European Nuclear Conference in Lyon, France, Sept. 23-28, 1990.

Hoffman, H., Fischer, H.D., Lochner, K.H., Mertens, U., "Microprocessor-based Information and Control Systems for Safety and Non-Safety Applications In Nuclear Power Plants of the Nineties," European Nuclear Conference, Lyon, France Sept. 23-28, 1990.

Hofmann, H.M., Jung, M., Konig, N., "BELT-D Offers Plant-Wide Integration of Digital I&C," *Nuclear Engineering International*, Vol. 34, No. 425, Dec. 1989.

Hofmann, H., "Cockpit Concept: Small and Simple", *Nuclear Engineering International*, July, (1989).

Hollnagel, E., and Woods, D. D., "Cognitive Systems Engineering, (New Wine in New Bottles)", in the *International Journal of Man-Machine Studies*, Vol. 18, pgs. 583-600, (1983).

Hoppe, P., Massier, H., Mitzel, F., Vath, W., "Untersuchungen zum Gaseintrag an KNK II", Institut fur Neutronenphysik und Reaktortechnik Projekt Schneller Bruter, November 1979.

IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," Approved April 5, 1972, American National Standards Institute.

"Implications of the Accident at Chernobyl for Safety Regulation of Commercial Nuclear Power Plants in the United States," Vol. 1, NUREG-1251.

Information presented to the panel by Mr. M. Combe and Mr. M. Montmayeul on 11/27/90 in handout, "Evolution of Operating System for Electronuclear Power Plants at EDF."

Informational handout received by the panel from CEGELEC entitled "CEGELEC in the Nuclear Field."

Interim Defence Standard 00-55, "Requirements for the Procurement of Safety Critical Software in Defence Equipment," Ministry of Defence, United Kingdom, May, 1988.

International Electrotechnical Commission Standard 880, "Software for Computers in the Safety Systems of Nuclear Power Plants," 1986.

Johnson, S. E., *DASS: A Decision Aid Integrating the Safety Parameter Display System and Emergency Functional Recovery Procedures*, EPRI NP-3595, August, 1984.

Jokineva, H., M. Lilja, and A. Sorenssen, "Early Fault Detection in a Real Nuclear Power Plant by Simulation Methods," ENC-90 paper no. 26/42.09, published in the Transactions of the ENS-90 Conference, pp. 1777-1781.

Kiessler, F.J., Hellmerich, K., and Schramm, W.,"Modernizing Reactor Protection," *Nuclear Engineering*, Vol. 34, 1989.

Kondratiev, V. V., Prozorov, V. K., "Effect of I&C Cable Ageing on Nuclear Reactor Safety."

Krcek, V., and Leicman, J., "Developing and Upgrading Full-Scope Systems in Czechoslovakia," *Nuclear Engineering International*, July 1990, p. 48.

Krogsaeter, M., Larsen, J. S., Nilsen, S., W. R. Nelson, and F. Owre, "Computerised Procedures--the COPMA System--and Its Proposed Validation Program," Expert Systems Applications in the Electric Power Industry, Orlando EPRI Conference, 1989.

Krogsaeter, M., Larsen,J.S., Nilsen, S., and Owre, F., "The Computerized Procedure System COPMA and its User Interface," International Atomic Energy Agency Specialist Meeting on Artificial Intelligence in Nuclear Power Plants, Helsinski, Finland, October 1012, 1989.

Lapassat, A., "Real Time Systems Software Validation and Verification," International Logistics Engineering Seminar, Dubrovnick, Yugoslavia, August, 1987.

Leroy, J.L., Millot, J.P., and Troublè, M. "Control Rod Cluster Assembly Command Method For Load Following PWRs Without Using Boration Changes", International Conference on the Physics of Reactors: Operation, Design and Computation, April 23- 27, 1990. Marseille, France.

Lipsett, J. J., Olmstead, R. A., Stevens, J. E. S., "Balancing the Roles of Humans and Machines in Power Plant Control", AECL-9955, presented to International Atomic Energy Agency Advisory Group Meeting on the Balance Between Automation and Human Actions, Vienna, Austria, 17-21 April, (1989).

Lupton, L. R., Lipsett, J. J., and Shah, R. R., "A Framework for Operator Support Systems for CANDU", presented at IAEA/NNPCI Specialists Meeting on Artificial Intelligence in Nuclear Power Plants, Helsinki, Finland, 10-12 October, (1989).

Lupton, L. R., Lipsett, J. J., Olmstead, R. A., Davey, E. C., "A Foundation for Allocating Control Functions to Humans and Machines in Future CANDU Nuclear Power Plants", presented at the IAEA/NEA International Symposium on Balancing Automation and Human Actions in Nuclear Power Plants, Munich, Federal Republic of Germany, 9-13 July, (1990).

Malkin, S.D., "NPP Automatization Concepts and Problems." Preprint IAE N4835/4, Moscow, 1989.

Malkin, S.D., Sivokon V.P., Chromov, V.K., Poznjakov, V.V. "Technical Solution of NPP Sabotage Invulnerability Problem." IAEA-SM-315/14, Munich, 9-13 July 1990.

Malkin, S.D., Sivokon V.P., Shmatkova L.V. "Quantitative Evaluation of a Fault Tolerance of Saftey Related NPP Systems." Soviet Atomnaja Energija, V.66, N1, 1989.

Marshall, E., C. Reiersen, and F. Owre, "Operator Performance with the HALO II Advanced Alarm System for Nuclear Plants--A Comparative Study," contained in Majumdar, C., D. Majumdar, and J. Sackett, *Artificial Intelligence and Other Innovative Computer Applications in the Nuclear Industry*, Plenum Press, New York, 1988.

Miles, J.B., "4GLs and CASE," *Government Computer News*, January 7, 1991, p. 49.

Mitzel, F., Vath, W., Ansari, S., "Nachweis von Brennelementschwingungen in KNK II", Institut fur Neutronenphysik und Reaktortechnik Projekt Schneller Bruter, November 1982.

"Mochovice I&C Contract Goes to KWU," *Nuclear Engineering International,* p. 3 (November, 1990).

Montmayeul, R., Lestien, A., Dien, Y., Bozec, J., "Two Aspects of the Technical and Ergonomical Evaluation of the Advanced Control Room of the New French PWR Units", Specialists' Meeting on the Human Factor Information Feedback in Nuclear Power: Implication of Operating Experience on System, Analysis, Design and Operation, Roskilde, Denmark, 25-27 May, (1987).

Mourlevat, J.L., Parry, A., et al., "Instrumentation and Control Revamping," *Fission Reactors*, March 13, 1990.

Naventi, R., "Documentation of Safety Software Systems for Reliability and Qualification," International Atomic Energy Agency Specialist Meeting on Software Reliability for Computerized Control and Safety in Nuclear Power Plants, Pittsburgh, Pennsylvania, July 20-22, 1977.

"NRC Action Plan Developed as a Result of the TMI-2 Accident," Vol. 1, NUREG-0660, May 1980.

Ness, Eyvind, Berg, Qivind, Sprenson, Aimar, "Early Detection and Diagnosis of Plant Anomalies Using Parallel Simulation and Knowledge Engineering Techniques," OECD Halden Reactor Project, paper given to the panel on 12/5/90.

Nikolayenko, V.A., Kurchatov Institute of Atomin Energy, Kurchatov Sq., 123182, Moscow, U.S.S.R. (personal communication).

Norman, D. A., *The Psychology of Everyday Things*, Basic Books, New York, (1988).

Nucleonics Week, Vol. 32, No. 1 (January 3, 1991).

NUREG-0308, "Safety Evaluation Report related to Operation of Arkansas Nuclear One, Unit 2," U.S. Nuclear Regulatory Commission, Docket No. 50-368, November 1977.

NUREG-0308, "Safety Evaluation Report related to Operation of Arkansas Nuclear One, Unit 2, Supplement Number 2," U.S. Nuclear Regulatory Commission, Docket No. 50-368, September 1978.

NUREG-0308, "Safety Evaluation Report related to Operation of Arkansas Nuclear One, Unit 2, Supplement Number 1," U.S. Nuclear Regulatory Commission, Docket No. 50-368, June 1978.

Olmstead, R. A., Fenton, E. F., "The Advanced CANDU Single Unit Control Room", presented at the International Conference on Availability Improvements in Nuclear Power Plants, Madrid, Spain, 10-14 April, (1989).

Owre, F., and Nilsen, S., "Integration Of A Real Time Expert System And A Modern Graphic Display System In A Swedish Nuclear Power Plant Control Room," *Expert Systems With Applications,* December, 1990.

Pain, C., Guesnier, G., Guilmin, J., "The Control Room and the Test Simulator", *Revue Generale Nucleaire*, No. 2, March-April, (1987). (An entire issue devoted to "The Command-Control Structure of the Units of the N4 Model", (in French)).

Papin, B., and Soldermann, R., "Display of Accident Operating Conditions Procedures Based on Generatized State Approach for Computerized Control Rooms." Paper received by the panel on 11/28/90.

Papin, B., P. Bernard, J. Tyran, G. Zwingelstein, and P. Bajard, "On Line Surveillance of Pressurized Water Reactors by Process Analysis," presented at the ANS Conference on Applications of Computers in Nuclear Power, Pasco, 1986.

Papin, B., Poujol, A., Beolet, M., Beltranda, "An Advanced Concept for Nuclear Plant Hierarchical Control: SYCOMORE." Paper given to the panel on 11/28/90.

Parry, A., Manager, Instrumentation and Control Department, Framatome, Tour Fiat - Cedex 16, 92084 Paris LaDefense, France (personal communication).

Parry, A., "Nuclear Power Plant I&C: A Modern Concept."

Pew, R. W., Miller, D. C., Feeher, C. E., *Evaluation of Proposed Control Room Improvements Through Analysis of Critical Operator Decisions*, Electric Power Research Institute NP-1982, (1981).

Pilaud, E., "Development and Qualification of Core Protection and Control System "CO3" For N4 Type Reactors," Merlin Gerin, Safety Electronic Systems Department.

Poujol, A., Papin, B. (CEA), and Soldermann, R. (EDF), "Dynamic Synthesis of Emergency Operating Procedures Based on Generalized State Approach," IWRG on MMI, IAEA, Schliersee, RFA, October 18-20, 1988.

Raimondo, E., "Instrumentation and Control Revamping," International Conference on Operability of Nuclear Systems in Normal and Adverse Environments, Lyon, France, Sept. 18-22, 1989.

Rasmussen, J., *Information Processing and Human-Machine Interaction, An Approach to Cognitive Engineering*, Elsevier Science Publishing Co., Inc., (1986).

Rasmussen, J. and Vicente, K., "Cognitive Control Of Human Activities And Errors: Implications For Ecological Interface Design," Fourth International Conference on Event Perception and Action, Trieste, Italy, August 24-28, 1987.

Rasmussen, J. and Goodstein, L.P., Chapter 9, "Information Technology and Work," *Handbook of Human-Computer Interaction*, M. Helander (ed.), Elsevier Science Publishers B.V., North Holland, 1988.

Rasmussen, J. and Vicente, K., "Coping With Human Errors Through System Design: Implications For Ecological Interface Design," *International Journal Man-Machine Studies*, (1989) 431, 517-534.

Reason, J. T., *Human Error*, Cambridge University Press, New York, (1990).

Redmill, F.J., Dependability of Critical Computer Systems 2, *Guidelines produced by The European Workshop on Industrial Computer Systems, Technical Committee 7* (EWICS TC7), Elsevier Applied Science, 1988.

Regulatory Guide 1.152, "Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research.

Reinartz, S. J., and Reinartz, G., "Analysis of Team Behavior During Simulated Nuclear Power Plant Incidents", *Contemporary Ergonomics 1989, Proceedings of the Ergonomics Society's Annual Conference on "Ergonomics--Designing Progress"*, Megaw, E. D. (Ed.), (1989).

Rogovin, M. (Dir.), "Three Mile Island, A Report to the Commissioners and to the Public", Nuclear Regulatory Commission Special Inquiry Group, U.S. Nuclear Regulatory Commission, (1981).

Rovene, L. A. (U. of Tenn.), Otoday, P. J., and Brittain, C. R. (ORNL), "Development of a Robust Model-Based Reactivity Control System," Canadian Nuclear Society Third International Conference on Simulation Methods in Nuclear Engineering, Montreal, Canada, 18-20 April 1990.

Sackett, J., Planchon, P., Sun, B., Williams, J. G., White, J. D., Beltracchi, L., Upadhyaya, B. R., Woods, D. D., *European Nuclear Instrumentation, Control, and Safety Technology*, National Science Foundation, (1989).

Saglietti, F., "Strategies for the Achievement and Assessment of Software Fault-Tolerance," 11th IFAC World Congress, Automatic Control in the Service of Mankind, Tallin, Estonia, USSR, August 13-17, 1990.

Saglietti, F., "Software Diversity Metrics Qualifying Dissimilarity in the Input Partition," *Software Engineering Journal*, Vol 5, No. 1, January 1990.

Saglietti, F., The Impact of Voter Granularity in Fault Tolerant Software on System Reliability and Availability," Fault Tolerant Computing System, Automation Systems, Methods, Application Systems, Methods, Applications, 4th International GI/ITG/GMA Conference, Baden-Baden, Germany, September 20-22, 1989.

Saglietti, F., "Optimal Combination of Software Testing Strategies," *Safety of Computer Control Systems 1988, Proceedings of the IFRAC Symposium*, Fulda, Germany, November 9-11, 1988.

Schleisiek, K., "Development of 'Smart' Sensors and Intelligent Signal Processing Methods", KFK Institute for Reactor Development, 1990 (personal communication).

Sheridan, T. B., "Understanding Human Error and Aiding Human Diagnostic Behaviour in Nuclear Power Plants", *Human Detection and Diagnosis of System Failures, Proceedings of a NATO Symposium*, Rasmussen, J. and Rouse, W. B. (Editors) pgs. 19-35, (1981).

Siemens, "Vibration Monitoring System", KWU Group.

Siemens, "Ultra-Sonic Liquid Level Monitoring", Power Generation Group.

Siemens, "Acoustic Leakage Monitoring System", Power Generation Group.

Siemens-KWU Picked for Mohovce I&C Replacement, *Nucleonics Week*, Vol. 31, No. 41, Oct. 11, 1990.

Stirsky, P., "National Report on Nuclear Power Plant Control and Instrumentation in Czechoslovakia," International Working Group on Nuclear Power Plant Control and Instrumentation/ING-NPPCI-IAEA/Munich, October 1982.

Streicher, V., Jax, P., Wehling, H.J., "Recently Developed KWU Systems For Monitoring Fatigue, Vibrations, Leakages and Loose Parts In Reactor Circuits", *IAEA CN-49/91, Proceedings of Man-Machine Interface in the Nuclear Industry Conference*, Tokyo, 15-19 February 1988.

Suzudo, T. and O. Berg, "On-Line Fault Size Estimation and Prognosis--An Operator Support System Demonstrated for the NORS Feedwater Preheaters," Halden Report HWR-236, April, 1989.

Tallec, M. Division D'Electronique, De Technology Et D'Instrumentation, Centre D'Etudes Nucleaires De Saclay - F 91191 Gif-Sur-Yvette Cedex, France.

Tetreau, F., Parry, A., "Instrumentation and Control Revamping," Framatome Nuclear Products and Services Technical Bulletin.

Tsventanov, R., Pashchenko, F. F., and Kolev, N. P., "Algorithms for Estimation of Assembly-wise Power Distribution in VVER Type Reactors." Paper given to the panel on 12/4/90.

U.S. Nuclear Regulatory Commission, "Human Factors Evaluation of Control Room design and Operator Performance at TMI-2", U.S. Nuclear Regulatory Commission NUREG/CR-1270, (1981).

Vath, W., Mitzel, F., Ansari, S. "Identification of Vibrational Effects in KNK II Fuel Elements", Institut fur Neutronenphysik und Reaktortechnik Projekt Schneller Bruter, July 1981.

Werner, Aleite, "Leittechnik Systems in Nuclear Power Plants and Their Importance to Reactor Safety," *Atomkernenergie Kerntechnik*, Vol 45, No. 4, pp 219-229, 1984.

Wilson, C., "Gettin GUI," *Workstation News*, pg. 28, November, 1990.

Woods, D. D., Wise, J. A., Hanes, L. F., *Evaluation of Safety Parameter Display Concepts*, Electric Power Research Institute NP-2239, (1982).

Yakimov, S.S., "Sensor Diagnostics of Hydrogen In Nuclear Power", Kurchatov Institute of Atomic Energy, Moscow USSR."

Zinser, K., "Design Issues and Knowledge Representations for Modern Control Room Interfaces", Proceedings of the IFAC Workshop Clyne Castle, Swansea, UK, 21-23 September 1988, International Federation of Automatic Control, (1988).